PÓŁROCZNIK NAUKOWY
PRAWO MEDIÓW ELEKTRONICZNYCH

Redakcja:
Redaktor naczelny – prof. dr hab. Jacek Gołaczyński
Sekretarz redakcji – dr Dariusz Szostek
Redaktor numeru – dr Marek Leśniak

Rada programowa:
dr Marek Świerczyński, UKSW
dr Wojciech Wiewiórowski, UG
dr Grzegorz Sibiga, INP PAN
prof. dr. Andreas Wiebe, University of Göttingen
adwokat Xawery Konarski
dr hab. prof. nadzw. UWr. Włodzimierz Gromski
dr hab. prof. nadzw. UWr. Krzysztof Wójtowicz
prof. dr hab. Ryszard Jaworski, UW
radca prawny Jacek Wilczewski,
Kancelaria Prawna Grynhoff Woźny Wspólnicy
adwokat Artur Kmieciak
sędzia Jacek Czaja

Recenzenci:
dr hab. prof. UKSW Grażyna Szpor
dr hab. prof. nadzw. UMK Andrzej Adamski
dr hab. prof. UOp Piotr Stec,
dr hab. prof. UŚ Jacek Górecki,
dr hab. prof. nadzw. UŁ Sławomir Cieślak
prof. Richard Warner, Ph.D, IIT Chicago-Kent College of Law
dr hab. prof. UJ Ryszard Markiewicz
prof. em. dr. Wolfgang Kilian, University of Hanover
dr hab. prof. UŚ Kazimierz Zgryzek

Korekta językowa:
dr Agnieszka Kulik-Jęsiek

Okładka, skład i łamanie:
Kamil Ligienza

© Copyright by Uniwersytet Wrocławski Wydział Prawa, Administracji i Ekonomii, Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej,
ul. Uniwersytecka 22/26, 51-145 Wrocław

ISSN 2082-100X

Adres redakcji:
Uniwersytet Wrocławski Wydział Prawa,
Administracji i Ekonomii,
Centrum Badań Problemów Prawnych i Ekonomicznych
Komunikacji Elektronicznej,
ul. Uniwersytecka 22/26, 51-145 Wrocław
e-mail: ebiuletyncbke@prawo.uni.wroc.pl

Produkcja:
VNT Law & Communications Sp. z o.o.
ul. Norblina 84, 40-748 Katowice,
tel.: 32 352 42 00, faks: 32 352 42 01
mob.: 0 602 334 664 , 0 660 530 054
e-mail: vnt@vnt.com.pl, szkolenia@vnt.com.pl
www.vnt.com.pl

WPROWADZENIE

Szanowni Państwo,

Oddajemy w Państwa ręce drugi numer półrocznika naukowego Prawo Mediów Elektronicznych. Znajdziecie w nim Państwo atykuły autorstwa m.in.: prof. UO dra hab. Dariusza Szostka oraz dr Bereniki Kaczmarek-Templin pt.: „Elektroniczna identyfikacja podmiotów w projekcie Rozporządzenia Parlamentu Europejskiego i Rady w sprawie identyfikacji i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym", dr Agaty Jaroszek pt.: „Dziecko jako podmiot ochrony prawnej w projekcie rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych". W kolejnych pracach przedstawione zostały „Praktyczne aspekty sporządzania protokołu skróconego i stosowania adnotacji w protokole elektronicznym" autorstwa mgr Aleksandry Klich (Uniwersytet Szczeciński) oraz „Problematyka anonimowości w Sieci, czyli jak dotrzeć do podmiotu naruszającego prawo w Internecie" mgr Marcina Szurpickiego (Uniwersytet Wrocławski).

Zachęcam zatem do lektury
prof. dr hab. Jacek Gołaczyński

Zasady publikacji:

Redakcja prosi o przysyłanie materiałów do publikacji w biuletynie zarówno w formie elektronicznej: pocztą elektroniczną lub na dyskietkach, jak również w formie wydruku. Tekst powinien być podpisany własnoręcznie przez autora. Tekst powinien być sporządzony w formacie MS Word, z zachowaniem interlinii oraz marginesów szerokości 3 cm. Tekst nie powinien przekraczać 15 stron znormalizowanego formatu A-4. Redakcja zastrzega sobie możliwość dokonywania skrótów, poprawek stylistycznych, językowych interpunkcyjnych. Prosimy autorów o podawania także swoich adresów prywatnych, numerów telefonów, adresów poczty elektronicznej, tytułów naukowych, zajmowanych stanowisk lub pełnionych funkcji, a także adresów właściwych urzędów skarbowych, numerów kont bankowych tych urzędów oraz danych osobowych potrzebnych do deklaracji podatkowej. Artykuły i recenzje niesamodzielnych pracowników naukowych będą poddawane recenzji.

SPIS TREŚCI

SPIS TREŚCI

ARTYKUŁY

JACEK GOŁACZYŃSKI

ELEKTRONICZNE CZYNNOŚCI SĄDOWE

Przepisy Kodeksu postępowania cywilnego oraz innych ustaw przewidują już obecnie możliwość dokonywania czynności sądowych w formie elektronicznej. Pod pojęciem formy elektronicznej będę rozumiał, na potrzeby tego artykułu, zarówno przypadki posłużenia się przez sąd podpisem elektronicznym zwykłym (art. 3 pkt 1 ustawy o podpisie elektronicznym z 18 wrzenia 2001 r.), jak również kwalifikowanym podpisem elektronicznym, czyli według art. 3 pkt 2 powyżej cytowanej ustawy. Przepis art. 58 ust. 2 ustawy o podpisie elektronicznym przewiduje, że organy władzy publicznej zostały zobowiązane do umożliwienia odbiorcom usług certyfikacyjnych w terminie do 1 maja 2008 r. wnoszenie podań i wniosków oraz dokonywanie innych czynności w postaci elektronicznej, w przypadku gdy przepisy prawa wymagają składania ich w szczególnej formie lub według określonego wzoru. Nie ma wątpliwości, że do tych organów należy zaliczyć także sądy powszechne. Jednakże rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 24 lipca 2007 r. w sprawie warunków udostępniania formularzy i wzorów dokumentów w postaci elektronicznej, wydane na podstawie art. 58 ust. 3 ustawy o podpisie elektronicznym nie odnosi się do pism procesowych i formularzy wnoszonych w postepowaniu cywilnym[1].

Powyższe przepisy donosiły się jednak wyłącznie do czynności procesowych. Podobnie jak przepis art. 125 k.p.c., który w brzmieniu sprzed nowelizacji dokonanej ustawą z 4 września 2008 r. stanowił, ze jeżeli przepis szczególny to przewiduje, pisma procesowe wnosi się na urzędowych formularzach lub na elektronicznych nośnikach informatycznych. Z kolei po noweli z 4 września 2008 r. zmieniono przepis art. 125 § 2 k.p.c. w ten sposób, że: jeżeli przepis szczególny tak stanowi, pisma procesowe wnosi się na urzędowych formularzach lub na informatycznych nośnikach danych albo za pośrednictwem środków komunikacji elektronicznej. Kolejna nowelizacja tego przepisu dokonana ustawą z dnia 9 stycznia 2009 r. o zmianie kodeksu postepowania cywilnego oraz niektórych innych ustaw przewidziała, że wnosi się na urzędowych formularzach lub za pośrednictwem systemu teleinformatycznego (droga elektroniczna) lub na informatycznych nośnikach danych[2]. W nowelizacji ustawy-Kodeks postepowania cywilnego, która jest obecnie przedmiotem prac rządowych (uzgodnienia międzyresortowe i konsultacje społeczne) przewidziano już jedynie możliwość wnoszenia pism procesowych za pośrednictwem systemu teleinformatycznego, jeżeli przepisz szczególny tak stanowi lub gdy strona dokonała wyboru wnoszenia pism za pośrednictwem tego systemu. Wraz z rozwojem technologii informatycznych głównym kanałem komunikacji pomiędzy strona postepowania a sądem jest zatem obecnie system teleinformatyczny.

Stąd też, *de lege lata*, nie jest dopuszczalne, aby strona wniosła pismo procesowe za pośrednictwem poczty elektronicznej i podpisała się bezpiecznym podpisem elektronicznym, czy nawet bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu. Kodeks postępowania cywilnego wyraźnie ograniczył sposób złożenia pisma procesowego jedynie do pośrednictwa systemu teleinformatycznego. W tej sytuacji pismo wniesione bez zachowania formy elektronicznej czynności procesowej[3], jaką jest podpis i system teleinformatyczny, powoduje skutek w postaci złożenia pisma. W przypadku elektronicznego postepowania upominawczego koniecznym warunkiem skutecznego złożenia pisma procesowego może być także opłata sądowa.

Projekt zmiany ustawy – kodeks postepowania cywilnego oraz innych ustaw, który jest przedmiotem prac legislacyjnych przewiduje zmianę art. 125 § 2 (1) przewiduje, że jeżeli przepis szczególny tak stanowi albo dokonano wyboru sposobu wnoszenia pism w sprawie za pośrednictwem systemu teleinformatycznego, pisma procesowe wnosi się wyłącznie za pośrednictwem tego systemu. Pisma niewniesione w ten sposób nie wywołują skutków prawnych, jakie ustawa wiąże z wniesieniem pisma do sądu, o czym sąd poucza wnoszącego pismo. W razie wniesienia pisma do sądu bez pośrednictwa systemu teleinformatycznego przewodniczący odsyła pismo wnoszącemu, zawiadamiając go o bezskuteczności czynności. Jednocześnie przepis art. 125 § 2 (2) projektu k.p.c. przewiduje, że powyższej reguły nie stosuje się, jeżeli nie względów technicznych nie było możliwe złożenie pisma procesowego za pośrednictwem systemu teleinformatycznego. Dotyczy to dwóch sytuacji, czyli, gdy pismo procesowe nie może być wniesione za pośrednictwem tego systemów z uwagi na względy techniczne i wówczas wnoszący pismo może to uczynić droga tradycyjna, czyli w formie pisemnej. Można tez ten przepis rozumieć w ten sposób, ze termin na dokonanie takiej czynności procesowej jest zawieszony do chwili powstania technicznych możliwości wniesienia pisma za pośrednictwem systemu. Skoro przepis par. poprzedzającego wskazuje, ze w razie np. wyboru sposobu wnoszenia pism w sprawie za pośrednictwem systemu teleinformatycznego, pismo wnosi się wyłącznie za pośrednictwem tego systemu, to brak jest podstaw do wniesienia pisma w formie pisemnej, a par. 2 (2) stanowi jedynie, ze termin do wniesienia pisma procesowego zostanie przedłużony okres występowania awarii technicznej.

Kolejnym przepisem projektowanym w nowelizacji Kodeksu postepowania cywilnego, który odnosi się do pism procesowych

[1] S. Kotecka, Akty prawne dotyczące informatyzacji postępowania cywilnego, w: Informatyzacja postępowania sadowego i administracji publicznej, red. J. Gołaczyński, Warszawa 2010r., s. 5

[2] Dz. U. Nr 26, poz. 156

[3] A. Kosiółek, Elektroniczne czynności procesowe w sądowy7m postepowaniu cywilnym, Warszawa 2012, s.

jest art. 126 par. 5 k.p.c. Stanowi on, ze pismo procesowe wniesione za pośrednictwem systemu teleinformatycznego opatruje się bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu lub podpisem elektronicznym potwierdzonym profilem zaufanym Elektronicznej Platformy Usług Administracji Publicznej. Przewiduje się zatem odejście od koncepcji posługiwania się stron zwykłym podpisem elektronicznym, jak w przypadku wnoszenia pism procesowym w elektronicznym postępowaniu upominawczym, czy w postępowaniu rejestrowym o rejestracje spółki z o.o. na podstawie ustawowego wzorca umowy (s-24). Nie oznacza to, że przepis art. 126 § 5 k.p.c. w wersji zawartej w projekcie, będzie miał charakter uniwersalny i zastąpi regulacje szczególne zawarte w art. 505 (30) k.p.c.[4]. Po wejściu w życie tej nowelizacji w każdym postepowaniu cywilnym poza elektronicznym postepowaniu upominawczym i postępowaniu rejestrowym dotyczącej spółki z o.o. zakładanej na podstawie ustawowego wzorca umowy, stosować będziemy bezpieczny podpis elektroniczny wersyfikowany przy pomocy ważnego kwalifikowanego certyfikatu.

Przechodząc do czynności sądowych należy zwrócić uwagę, że dotychczasowe regulacje wyraźnie wskazują pisemność czynności sądowych, a zwłaszcza orzeczeń sądowych. Wyrok składa się z sentencji i uzasadnienia, o ile strona wystąpi z wnioskiem o jego sporządzenie. W Przypadku postępowania apelacyjnego, uzasadnienie sporządzane jest także z urzędu w razie zmiany lub uchylenia zaskarżonego wyroku. Gdy apelacja została oddalona Sąd Apelacyjny sporządza uzasadnienie na wniosek strony. Sposób sporządzenia wyroku reguluje przepis art. 324 k.p.c. W §ie 1 przewiduje, że wyrok sporządza się po niejawnej naradzie sędziów. Narada obejmuje, głosowanie nad mającym zapaść orzeczeniem i zasadniczymi powodami rozstrzygnięcia oraz spisanie sentencji wyroku. § 2 tego artykułu stanowi następnie o sposobie zbierania głosów przewidując, że głosy zbiera się od sędziów według ich starszeństwa służbowego, a ławników według ich wieku, poczynając od najmłodszego, sam zaś głosuje ostatni. Sprawozdawca, jeżeli jest wyznaczony głosuje pierwszy. Wyrok zapada większością głosów. Sędzia, który przy głosowaniu nie zgodził się z większością, może przy podpisywaniu sentencji zgłosić zdanie odrębne i obowiązany jest uzasadnić je na piśmie przed podpisaniem uzasadnienia. Sentencję wyroku podpisują jednak wszyscy sędziowie, czy sędziowie i ławnicy (§ 3 art. 324 k.p.c.)[5].

Obecnie przepis ten odrywa istotną rolę w postępowaniu, w którym występuje skład wieloosobowy sądu, czyli w sprawach rodzinnych, pracowniczych, rozwodowych i apelacyjnych. W zdecydowanej jednak większości w postępowaniu przed sądami pierwszej instancji skład sądu jest ograniczony do jednego sędziego zawodowego. Z punktu widzenia sposobu, w jaki może być złożony podpis, przepis art. 324 k.p.c. nie budzi wątpliwości, że sentencja wyroku winna być podpisana przez cały skład sądu, czyli przewiduje się tutaj dla zachowania wymogu formy – podpisy własnoręczne. Zachodzi zatem pytanie, czy w przypadku sporządzenia wyroku w postaci elektronicznej, która jest równoważna formie pisemnej zgodnie z art. 78 § 2 k.c. już teraz jest możliwe sporządzenie sentencji wyroku w formie elektronicznej. Przepisy, które przewidują możliwość sporządzenia orzeczenia sądu w formie elektronicznej ograniczone są jedynie do orzeczenia w postępowaniu rejestrowym i w elektronicznym postępowaniu upominawczym i dotyczą zarówno samego nakazu zapłaty, jak i postanowienia sądu o nadaniu klauzuli wykonalności takiemu tytułowi egzekucyjnemu. Z przepisu art. 324 k.p.c. wynika bowiem, że sentencja winna być sporządzona na piśmie. Zasada pisemności należy do jednej z podstawowych zasad postępowania cywilnego i dotyczy zarówno czynności procesowych stron, jak i czynności sadowych w tym orzeczeń. Pisemność jednak, posługując się dorobkiem prawa cywilnego materialnego, nie zawsze oznacza, że musimy użyć podpisu własnoręcznego. Możliwe jest także wykorzystanie podpisu elektronicznego, który zgodnie z prawem jest równoważny podpisowi własnoręcznemu. I tak, przepis art. 78 § 2 k.c. przewiduje, że oświadczenie woli może być podpisane także podpisem elektronicznym bezpiecznym, weryfikowanym ważnym kwalifikowanym certyfikatem. Jedynie w takim przypadku uzyskuje skutek równoważny zwykłej formy pisemnej. Należy pamiętać także, że przepis ten odpowiada art. 5 dyrektywy o podpisie elektronicznym, według którego dane w postaci elektronicznej opatrzone bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego certyfikatu są równoważne pod względem skutków prawnych dokumentom opatrzonym podpisami własnoręcznymi, chyba że przepisy odrębne stanowią inaczej. Dominuje przekonanie w doktrynie prawa cywilnego, że przepis ten ma zastosowanie szersze niż tylko do prawa cywilnego, czyli czynności prawnych, ponieważ odnosi się do wszelkich danych, w tym także niewyrażających oświadczeń woli. Przepis art. 6 ustawy o podpisie elektronicznym zrównuje każdy dokument elektroniczny z każdym dokumentem pisemnym, chyba, ze z przepisów szczególnych wynika cos innego. Przepis art. 78 § 2 k.c. jest właśnie takim przepisem odrębnym i dlatego ustawodawca polski zawęził zastosowania art. 5 ustawy o podpisie elektronicznym w zakresie formy czynności prawnych jedynie do tych czynności, które są dokonywane w formie pisemnej zwykłej. Nie odnosi się zatem i nie rodzi równoważnego skutku forma o której mowa w art. 78 § 2 k.c. dla czynności prawnej wyrażanej w szczególnej formie pisemnej[6].

Stąd powstaje pytanie, czy obecnie na gruncie przepisów kodeksu postępowania cywilnego jest dopuszczalne sporządzenie sentencji wyroku w formie elektronicznej? Dla odpowiedzi na takie pytanie, konieczne jest ustalenie, czy przepis art. 5 ustawy o podpisie elektronicznym odnosi się do czynności procesowym w postępowaniu cywilnym i czynności sądowych w tym postępowaniu. W tym pierwszym przypadku należy przyjąć, że jedynie wówczas, gdy przepisy kodeksu postępowania cywilnego dają możliwości dokonania czynności procesowej za pośrednictwem środków komunikacji elektronicznej. Taka sytuacja zachodzi odnośnie do czynności procesowych. Cytowany już powyżej przepis art. 125 k.p.c. przewiduje możliwość dokonania czynności procesowej wyłącznie za pośrednictwem systemu informatycznego, o ile przepis szczególny tak stanowi. Dotyczy to zatem jedynie elektronicznego postępowania upominawczego i postepowań rejestrowych w zakresie wpisów do Krajowego Rejestru Sądowego i rejestru zastawów. Nie ma obecnie innej podstawy dla dokonania czynności procesowej elektronicznie.

[4] B. Kaczmarek, w: Elektroniczne postepowanie upominawcze. Komentarz, (red. J. Gołaczyński), Warszawa 2010, s. 167.

[5] A. Góra-Błaszczykowska, w: Kodeks postępowania cywilnego. Tom I. Komentarz, Warszawa 2013, (red. A. Góra Błaszczykowska), s. 708 i n.

[6] K. Górska, Zachowanie zwykłej formy pisemnej czynności prawnych, Warszawa 2007, s. 225 i cyt. Tam lit.

Te same uwagi odnoszą się do czynności sądowej. W kodeksie postępowania cywilnego jedynie w elektronicznym postępowaniu upominawczym i postępowaniu rejestrowym sąd może (w składzie sędziowskim, czy referendarskim) sporządzić czynność sądowa w formie elektronicznej. To dotyczy także orzeczeń sądowych. Skoro przepis art. 5 ustawy o podpisie elektronicznym przewiduje zrównanie dokumentu pisemnego z elektronicznym opatrzonym bezpiecznym podpisem elektronicznym weryfikowanym ważnym kwalifikowanym certyfikatem, o ile przepis szczególny nie stanowi inaczej, to oznacza, że nie jest dopuszczalne sporządzenie czynności sądu w innym przypadku, niż to wynika z przepisu szczególnego.

Obecnie zatem sentencja wyroku nie może być podpisana bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu i tym samym nie zastąpi sentencji podpisanej własnoręcznie przez skład sądu[7].

Nie dotyczy to nakazu zapłaty wydanego w elektronicznym postepowaniu upominawczym, w którym sąd może jedynie w formie elektronicznej wydać taki nakaz posługując się bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu. Projekt nowelizacji Kodeksu postępowania cywilnego przewiduje w tym zakresie także dalsze zmiany mające na celu umożliwienie także w innych postepowaniach wydawania orzeczeń sadowych w formie elektronicznej. W pierwszej kolejności należy to wymienić art. 677 do którego dodaje się par. 4, który stanowi, że: „za pośrednictwem systemu teleinformatycznego, prezes sądu albo osoba przez niego wyznaczona dokonuje niezwłocznie wpisu prawomocnego postanowienia o stwierdzeniu nabycia spadku do Rejestru Spadkowego prowadzonego przez Krajową Radę Notarialną. Prezes Sądu lub wyznaczona przez niego osoba opatruje wpis bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu. Postanowienie sądu w sprawie o stwierdzenie nabycia spadku wydawane jest zatem w formie pisemnej, natomiast informacja o treści postanowienia skierowana do rejestru Spadkowego wymaga już formy elektronicznej kwalifikowanej z uwagi a to, że rejestr ten ma być prowadzony, podobnie jak obecnie Rejestr Poświadczeń Dziedziczenia, elektronicznie.

Z mocy projektowanego art. 759 (12) k.p.c. także komornik sądowy będzie mógł utrwalać swoje czynności w systemie teleinformatycznych i wówczas jego czynności winny być opatrywane bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu (art. 3 pkt 2 ustawy o podpisie elektronicznym z 18 września 2001r).

Kolejnym przykładem wykorzystanie formy elektronicznej orzeczeń sadowych jest projektowany w nowelizacji kodeksu postepowania cywilnego przepis art. 781 § 3 (1) k.p.c., który przewiduje, że czynności sądu, referendarza sadowego i przewodniczącego są utrwalane wyłącznie w systemie teleinformatycznym, a wytworzone w ich wyniku dane w postaci elektronicznej opatrywane są bezpiecznym podpisem elektronicznym w rozumieniu art. 3 pkt 2 ustawy o podpisie elektronicznym z dnia 18 września 2001 r. Podobnie rzecz się ma z postanowieniem sądu o nadaniu klauzuli wykonalności.

Powstaje zatem pytanie, czy w przypadku wejścia w życie nowelizacji Kodeksu postepowania cywilnego, która będzie przewidywał wybór wnoszenia pism procesowych za pośrednictwem systemu teleinformatycznego nie należy przewidzieć w tych sprawach także orzeczenia sadowego wydanego w formie elektronicznej. W sytuacji, gdy orzeczenie zostanie wdane na posiedzeniu niejawnym w pierwszej instancji, w sprawach, w których skład sadu składa się z jednego sędziego, posłużenie się forma elektroniczna orzeczenia nie będzie nastręczało większych problemów technicznych i organizacyjnych. Podobnie bowiem jak w elektronicznym postępowaniu upominawczym orzeczenie sądowe byłoby wydawane w systemie teleinformatycznym i przybierałoby formę elektroniczną. Konieczne jest opatrywanie takiego orzeczenia bezpiecznym podpisem elektronicznym, o którym mowa w art. 3 pkt 2 ustawy o podpisie elektronicznym. Dotyczyłoby to nakazu zapłaty w postępowaniu nakazowym, nakazu zapłaty w postepowaniu upominawczym, postanowień o nadaniu klauzuli wykonalności tytułom egzekucyjnym, oraz orzeczenia o charakterze incydentalnym, jak postanowienie o zwolnieniu od kosztów sadowych, ustanowienie adwokata z urzędu itd.

W przypadku, gdy w toku postepowania sąd wydaje orzeczenie po przeprowadzeniu rozprawy, należy także zauważyć, że w sprawach rozpoznawanych w składzie jednoosobowym, nie ma technicznych, ani organizacyjnych przeszkód, aby sąd wydawał wyrok (postanowienie co do *meritum* w postępowaniu nieprocesowym), w formie elektronicznej. Wyrok jednak winien być, stosownie do art. 324 k.p.c. podpisany, a konkretnie jego sentencja. Podpisanie wyroku może być dokonane przy użyciu bezpiecznego podpisu elektronicznego weryfikowane przy pomocy kwalifikowanego certyfikatu. Następnie, zgodnie z art. 326 k.p.c. przewodniczący winien ogłosić wyrok. Nie ma zatem, w moim przekonaniu żadnych przeszkód prawnych, aby przenieść rozwiązanie ze zwykłego postępowania cywilnego, do tego, w którym strony wybrały wnoszenie pism procesowych za pośrednictwem systemu teleinformatycznego. Jedyna różnica, która tu będzie występowała, to rodzaj podpisu złożonego rzez sędziów. W miejsce własnoręcznego, podpis elektroniczny. Orzeczenie wydane w taki sposób zostałoby przybierałoby formę elektroniczną. Niewątpliwą zaletą takiego rozwiązania będzie większa dostępność informacji o wydanym orzeczeniu. W postępowaniu inicjowanym przez stronę w systemie teleinformatycznym dostęp do akt sprawy odbywa się za pośrednictwem konta założonego w systemie teleinformatycznych utworzonym dla obsługi tego postępowania. Strona, podobnie jak w elektronicznym postępowaniu upominawczym, mogłaby samodzielnie wydrukować wydruk takiego orzeczenia wprost z tego systemu teleinformatycznego (repozytorium elektronicznego), a następnie inny sąd, niż ten, który wydał orzeczenie mógłby weryfikować istnienie tego tytułu egzekucyjnego w systemie teleinformatycznych obsługującym to postępowania. Kolejną zaletą elektronicznej formy tytułu egzekucyjnego jest możliwość nadania takiemu tytułowi klauzuli wykonalności w formie elektronicznej. Obecnie taka sytuacja jest możliwa w elektronicznym postępowaniu upominawczym, zgodnie z art. 783 § 4 k.p.c. Z § 4 ust. 1 rozporządzenia Ministra Sprawiedliwości z dnia 28 grudnia 2009 r. w sprawie czynności sądu związanych z nadawaniem klauzuli wykonalności orzeczeniu sądowemu wydanemu w elektronicznym postepowaniu

[7] Por. orz. SN z 26 marca 2009r. I KZP 39/08, gdzie Sąd Najwyższy uznał, za niedopuszczalne wniesienie apelacji w postepowaniu w sprawach o wykroczenia w formie elektronicznej z podpisem bezpiecznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu.

upominawczym[8] wynika, że sąd lub referendarz sądowy wydaje postanowienie o nadaniu klauzuli wykonalności nakazowi zapłaty w elektronicznym postępowaniu upominawczym w systemie teleinformatycznym opatrując je bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu. Jednocześnie rozporządzenia nakłada na sąd obowiązek umieszczania elektronicznego tytułu wykonawczego w repozytorium, czyniąc o tym wzmiankę w aktach sprawy (także w formie elektronicznej[9]). § 5 przewiduje natomiast dostęp dla podmiotów wskazanych w przepisach odrębnych do tego repozytorium oraz umożliwienie im wydruku weryfikacyjnego takiego tytułu wykonawczego. W przypadku zaś wszczęcia egzekucji na podstawie tytułu wykonawczego istniejącego w formie elektronicznej, podobnie jak obecnie w przypadku elektronicznego postepowania upominawczego, zgodnie z art. 805 § 3 k.p.c., dłużnikowi okazuje się wydruk weryfikacyjny tytułu wykonawczego.

Komornik mógłby składać wniosek o wszczęcie egzekucji w sprawie, w której postepowanie było prowadzone za pośrednictwem systemu teleinformatycznego w formie elektronicznej. Takie rozwiązanie redukuje koszty postepowania egzekucyjnego oraz zmierza do jego większej szybkości.

Z art. 781 § 1 k.p.c. wynika, że sądem właściwym do nadania klauzuli wykonalności tytułom egzekucyjnym wydanym w elektronicznym postępowaniu upominawczym będzie sąd pierwszej instancji, w którym sprawa się toczy, czyli Sąd Rejonowy Lublin Zachód. Podobnie ten sąd będzie właściwy do nadania klauzuli wykonalności orzeczeniom wydanym w elektronicznym postepowaniu upominawczym nienależącym do kategorii wyłącznej art. 781 § 1 (2) k.p.c. Należy zatem rozważyć, czy w przypadku spraw, w których doszło do wydania orzeczenia w formie elektronicznej, innego niż nakazu zapłaty w elektronicznym postępowaniu upominawczym, każdy sąd mógłby nadać klauzulę wykonalności orzeczeniu. Akta sprawy są bowiem prowadzone w systemie teleinformatycznym, do którego każdy sąd miałby dostęp, jak obecnie do spraw rozpoznawanych w elektronicznym postępowaniu upominawczym.

Po nadaniu nakazowi zapłaty klauzuli wykonalności wierzyciel może wszcząć egzekucję. Odrębność wynikająca z elektronicznego postępowania upominawczego polega na tym, że wniosek o wszczęcie egzekucji na podstawie tytułu wykonawczego, o którym mowa w art. 797 § 2-5 k.p.c., może być złożony także za pośrednictwem systemu teleinformatycznego obsługującego elektroniczne postępowanie upominawcze. W przypadku wszczęcia egzekucji na podstawie tytułu egzekucyjnego zaopatrzonego w klauzule wykonalności, pochodzącego z elektronicznego postępowania upominawczego, komornik ma obowiązek zweryfikować treść przedstawionego mu przez wierzyciela dokumentu uzyskanego z systemu teleinformatycznego oraz zaznaczenia w tym systemie faktu prowadzenia egzekucji na podstawie tego tytułu. Kwestia ta została uregulowana w art. 797 § 4 k.p.c. Istotne jest to, że wierzyciel, którego wierzytelność została stwierdzona nakazem zapłaty wydanym w elektronicznym postępowaniu upominawczym może dokonać wyboru, w jaki sposób złoży wniosek o wszczęcie egzekucji komornikowi. Może to bowiem uczynić tradycyjnie, czyli wniosek złożyć w postaci papierowej, i wtedy do tego wniosku należy dołączyć dokument z systemu teleinformatycznego, w którym prowadzone jest elektroniczne postępowanie upominawcze. Wierzyciel może jednak skorzystać z drogi elektronicznej, czyli za pośrednictwem systemu teleinformatycznego dedykowanego dla tego postępowania. Takie rozwiązanie może być także zastosowane w przypadku wydania orzeczenia sądowego w formie elektronicznej w innym postepowaniu, niż w elektronicznym postępowaniu upominawczym. Do wniosku lub żądania przeprowadzenia egzekucji z urzędu należy dołączyć wydruk weryfikacyjny, czyli dokument pochodzących z systemu teleinformatycznego, umożliwiający organowi egzekucyjnemu weryfikacje istnienia i treści tytułu egzekucyjnego (art. 797 § 3 k.p.c.). Oczywiście ten wydruk weryfikacyjny nie jest tytułem wykonawczym, ani nawet jego odpisem, a jedynie sposobem udokumentowania istnienia samego tytułu[10]. Należy podkreślić, że tytuł egzekucyjny oraz klauzula wykonalności znajduje się w systemie teleinformatycznym dedykowanym dla elektronicznego postępowania elektronicznego[11]. Pojęcie „wydruku weryfikacyjnego" zostało uregulowane w § 2 pkt 2 rozporządzenia Ministra Sprawiedliwości z dnia 28.12.2009 r. w sprawie czynności sądu związanych z nadawaniem klauzuli wykonalności orzeczeniu pochodzącemu z elektronicznego postępowania nakazowego. Komornik ma obowiązek zweryfikować treść przedstawionego dokumentu (uzyskanego z systemu teleinformatycznego) oraz zaznaczenie w systemie faktu prowadzenia egzekucji na podstawie tego tytułu (art. 797 § 4 k.p.c.).

Natomiast po ukończeniu postępowania egzekucyjnego należy na tytule wykonawczym zaznaczyć wynik egzekucji i tytuł zatrzymać w aktach, a jeżeli świadczenie objęte tytułem nie zostało zaspokojone całkowicie, tytuł zwrócić wierzycielowi. Jeżeli zaś egzekucja była prowadzona na podstawie tytułu wykonawczego, o którym mowa w art. 783 § 4 k.p.c. powyższe informacje komornik odnotowuje w systemie teleinformatycznym, w którym jest prowadzone elektroniczne postępowanie upominawcze (art. 816 § 2 k.p.c.). Kwestie te szczegółowo reguluje rozporządzenie Ministra Sprawiedliwości z dnia 23.12.2009 r. w sprawie szczegółowych czyn postaci Krajowej Rady Komorniczej oraz szczegółowych czynności komornika związanych z egzekucją prowadzoną na podstawie elektronicznego tytułu wykonawczego. Nie ma wątpliwości, aby to rozwiązanie, zaczerpnięte z elektronicznego postępowania upominawczego mogło być wykorzystane także w postepowaniu, w którym wydano orzeczenie w formie elektronicznej, inne niż nakaz zapłaty w elektronicznym postępowaniu upominawczym.

Należy się opowiedzieć, za wprowadzeniem na większą skalę czynności sądowych, w tym orzeczeń sadowych dokonywanych w formie elektronicznej. Najlepszym i sprawdzonym wzorcem mogą być liczne regulacje odnoszące się do elektronicznego postepowania upominawczego. One tworzą już teraz sprawnie działające narzędzie dla istnienia formy elektronicznej czynności sądowym, tak w postępowaniu rozpoznawczym, jak i egzekucyjnym.

[8] Dz. U. Nr 226, poz. 1833

[9] Rozporządzenie Ministra Sprawiedliwości z dnia 23 lutego 2007r. –Regulamin urzędowania sadów powszechnych(Dz. U. Nr 38, poz. 249 i z późn. zm). Z §ie 272a wynika, że akta sprawy w elektronicznym postępowaniu upominawczym prowadzone są w systemie teleinformatycznym. Dokumenty papierowe są skanowane i wprowadzane do akt elektronicznych, a następnie umieszczane w pomocniczym zbiorze dokumentów.

[10] D. Szostek, Nowe ujęci dokumentu oraz formy elektronicznej w prawie cywilnym, W: E. Gruza (red.), Dokument we współczesnym prawie, Warszawa 2009, s. 73; tenże, Nowe ujęcie dokumentu w prawie prywatnym, warszawa 2012, s.

[11] B. Pękalski, w: Elektroniczne postepowanie upominawcze. Komentarz, red. J. Gołaczyński, Warszawa 2010, s. 272

Abstract

In turn, Jacek Gołaczyński in the article "Electronic judicial acts" speaks in favor of a large-scale judicial acts, including – judicial decisions made in electronic form. As the best and proven model he considers all regulations relating to the electronic proceedings. According to the author, they have already formed an efficient tool for the operation of electronic judicial acts, both in the examination and enforcement proceedings.

DARIUSZ SZOSTEK, BERENIKA KACZMAREK-TEMPLIN

ELEKTRONICZNA IDENTYFIKACJA PODMIOTÓW W PROJEKCIE ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY W SPRAWIE IDENTYFIKACJI I USŁUG ZAUFANIA W ODNIESIENIU DO TRANSAKCJI ELEKTRONICZNYCH NA RYNKU WEWNĘTRZNYM

Od wielu lat w obrocie elektronicznym, zarówno odnoszącym się do transakcji prywatnych, jak również do usług publicznych, jednym z pojawiających się problemów jest identyfikacja podmiotów dokonujących czynności prawnych. Począwszy od uchwalenia dyrektywy o podpisie elektronicznym[2], przez szereg lat uważano, iż podstawową metodą identyfikacji powinien być kwalifikowany podpis elektroniczny weryfikowany ważnym kwalifikowanym certyfikatem (w znaczeniu dyrektywy 99/93/WE). Miał on służyć zapobieganiu anonimowości użytkowników oraz umożliwiać dokonywanie przy pomocy środków komunikacji elektronicznej czynności prawnych, które w obrocie tradycyjnym wymagają formy pisemnej[3]. W praktyce kwalifikowany podpis elektroniczny (w Polsce jest to bezpieczny podpis elektroniczny weryfikowany ważnym kwalifikowanym certyfikatem) nie znalazł szerokiego zastosowania. W praktyce, tylko tam gdzie Państwo ustawowo nakazało korzystanie z bezpiecznego podpisu elektronicznego ma on poważniejsze zastosowanie, w obrocie prywatno – prawnym jego znaczenie jest raczej marginalne. Użycie bezpiecznego podpisu elektronicznego jest wymagane tylko w przypadku ustawowo wskazanych usług opierających się o taką metodę identyfikacji (np. GIIF, ZUS itd.).

Jedną z przyczyn braku zainteresowania podpisem elektronicznym jest problem jego uznawalności w obrocie transgranicznym, i to zarówno wewnątrzwspólnotowym, jak i z państwami trzecimi.

Niestety, również w komunikacji obywateli z organami państwowymi (w tym organami wymiaru sprawiedliwości) bardzo utrudniona jest wymiana korespondencji w postaci elektronicznej. W ramach postępowań cywilnych, praktycznie poza elektronicznym postępowaniem upominawczym w ogóle nie jest możliwa. W postępowaniu administracyjnym elektroniczna komunikacja jest teoretycznie możliwa, a w praktyce – ze względu na brak możliwości konwertowania dokumentów istniejących tylko w postaci papierowej do postaci elektronicznej – bardzo utrudniona.

Często jako argument przeciwko możliwości elektronicznego przesyłania pism do sądów czy organów administracji, wskazuje się duże ryzyko, iż pisma będą składane przez osoby podszywające się za osoby wskazane jako ich autorzy[4].

Problem dotyczący identyfikacji podmiotów w czynnościach dokonywanych w postaci elektronicznej, w tym także w obrocie transgranicznym, został dostrzeżony na gruncie prawa wspólnotowego. Po dziesięciu latach obowiązywania dyrektywy 99/93/WE zarówno doktryna jak i praktyka zgodnie wskazują, iż jej regulacje nie są wystarczające, a nadto jej implementacje w poszczególnych systemach państw członkowskich wywołują wiele wątpliwości. Problem w uznawalności podpisów w obrocie transgranicznym, oraz także trudności w uznawalności dokumentów w postaci elektronicznej i przekonwertowanych do postaci elektronicznej dokumentów tradycyjnych, skłoniły Komisję Europejską do przygotowania projektu nowego aktu wspólnotowego, którego celem jest ujednolicenie elektronicznej identyfikacji podmiotów.

[1] COM(2012) 238 final 2012/0146 COD

[2] Dyrektywa Parlamentu Europejskiego i Rady Unii Europejskiej z dnia 13 grudnia 1999 w sprawie ramowych warunków Wspólnoty dla podpisu elektronicznego.

[3] Zob. szerzej Z. Radwański, Elektroniczna forma czynności prawnych, Monitor Prawniczy nr 22/2001, s. 18, tenże [w:] System prawa prywatnego pod red. Z. Radwańskiego, Warszawa 2002, s. 165; F. Wejman, Wprowadzenie do cywilistycznej problematyki ustawy o podpisie elektronicznym, Prawo Bankowe 2002, nr 4, s. 38; W. J. Kocot, Wpływ Internetu na prawo umów, Warszawa 2005, s. 347 i n.; tenże, Charakter prawny podpisu elektronicznego, PPH 2002, nr 4, s. 41; D. Szostek, Prawne aspekty podpisu elektronicznego [w:] Handel elektroniczny. Problemy prawne (red. J. Barta, R. Markiewicz), Kraków 2005, s. 175 i n.; tenże, Czynność prawna a środki komunikacji elektronicznej, Kraków 2004, s. 230 i n.; tenże, Podpis elektroniczny – problemy prawne, PPH 2002, nr 1; M. Świerczyński, Podpis elektroniczny [w:] Prawo Internetu (red. P. Podrecki), s. 63 i n.; K. Korus, Podpis elektroniczny [w:] Prawo handlu elektronicznego, Bydgoszcz – Kraków 2005, s. s. 22 i n.; M. Drozdowicz, (Nie)bezpieczny podpis elektroniczny, PPH 2003, nr 1, s. 30; M. Butkiewicz, Wpływ ustawy o podpisie elektronicznym na formę czynności prawnych, PPH 2003, nr 4, s. 32; D. Szostek, M. Świerczyński, The Conclusion of a Contract via the Internet in the Polish law [w :] Law of E-Commerce in Poland and Germany (red. B. Heiderhoff, G. Żmij), München 2005, s. 27-29; E. Wyrozumska, Elektroniczne oświadczenie woli w ustawie o podpisie elektronicznym i po nowelizacji kodeksu cywilnego, PPH 2003, nr 8, s. 50-51;M. Leśniak, Elektroniczna forma czynności prawnych [w:] Umowy elektroniczne w obrocie gospodarczym (red. J. Gołaczyński), Warszawa 2005, s. 78 i n.; B. Pabin, Elektroniczna forma czynności prawnych, Przegląd Prawa i Administracji, t. LXI, Wrocław 2004, s. 47 i n.; R. Podpłoński, P. Popis, Podpis elektroniczny. Komentarz, Warszawa 2004.

[4] Argumentacja jest taka o tyle nie trafna, iż w przypadku pism procesowych składanych w postaci papierowej sąd, czy też organ administracji, nie bada uprzednio podpisu i nie weryfikuje tożsamości osób wskazanych jako podmioty składające, a gremialnego podszywania pod autora pisma nie ma. Ewentualna kontrola tożsamości jest następcza, czyli dochodzi do niej w przypadku podejrzenia przestępstwa fałszowania dokumentu lub podszywania się pod inną osobę.

Do chwili obecnej, materia związana z identyfikacją podmiotów, zawarta była w dyrektywie nr 99/93/WE. Jednakże taka postać aktu prawnego nie zapewnia wdrożenia jednolitego rozwiązania na terenie całej Wspólnoty. Dyrektywy zwykle pozostawiają krajom członkowskim znaczną swobodę wyboru rozwiązań. Z tego też względu Komisja Europejska, dla zharmonizowania prawa wspólnotowego w tym zakresie, przedstawiła projekt Rozporządzenia Parlamentu Europejskiego i Rady w sprawie identyfikacji i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym[5].

W preambule wskazano główne powody przygotowania projektu rozporządzenia. Przede wszystkim jego celem „jest zwiększenie zaufania do transakcji elektronicznych na rynku wewnętrznym poprzez zapewnienie bezpiecznych i płynnych interakcji elektronicznych miedzy przedsiębiorstwami, obywatelami i organami publicznymi, co pozwoli podnieść skuteczność publicznych i prywatnych usług online, e-biznesu i handlu elektronicznego we Wspólnocie Europejskiej. Dyrektywa Parlamentu Europejskiego i Rady nr 1999/93/WE z dnia 13 grudnia 1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych obejmuje głównie podpisy elektroniczne, nie zapewnia natomiast szczegółowych ram transgranicznych i międzysektorowych, które odnosiłyby się do bezpiecznych, wiarygodnych i łatwych do realizacji transakcji elektronicznych. Projektowane rozporządzenie umacnia i jednocześnie poszerza dorobek doktrynalny i orzeczniczy tej dyrektywy.

W większości przypadków dostawcy usług z innego państwa członkowskiego nie mogą korzystać ze swojej identyfikacji elektronicznej w celu zapewnienia sobie dostępu do tych usług, ponieważ systemy identyfikacji elektronicznej w ich kraju nie są uznawane i akceptowane w innych państwach członkowskich. Taka bariera elektroniczna nie pozwala dostawcom usług w pełni korzystać z rynku wewnętrznego. Wzajemnie uznawane i akceptowane środki elektronicznej identyfikacji ułatwia transgraniczne świadczenie licznych usług na rynku wewnętrznym i umożliwia przedsiębiorstwom prowadzenie działań za granica bez konieczności zmagania się przeszkodami wynikającymi z kontaktów z organami administracji publicznej. Jednym z celów omawianego rozporządzenia jest zniesienie istniejących barier w transgranicznym stosowaniu środków identyfikacji elektronicznej stosowanych w państwach członkowskich w celu uzyskania dostępu przynajmniej do usług publicznych. Celem niniejszego rozporządzenia nie jest ingerowanie w systemy zarządzania tożsamością elektroniczna i w powiązane z nimi infrastruktury ustanowione w państwach członkowskich. Rozporządzenie ma służyć zagwarantowaniu bezpiecznej identyfikacji elektronicznej i bezpiecznego elektronicznego uwierzytelniania do celów korzystania z transgranicznych usług online oferowanych przez państwa członkowskie.

Wsparcie ogólnego transgranicznego korzystania z elektronicznych usług zaufania, wymaga zapewnienia możliwości używania ich jako dowodu w postepowaniach sądowych we wszystkich państwach członkowskich.

Z punku widzenia dalszego rozwoju transgranicznych transakcji elektronicznych na rynku wewnętrznym ważne jest również, by oryginalne dokumenty elektroniczne lub uwierzytelnione odpisy wydawane przez właściwe organy w państwie członkowskim zgodnie z przepisami krajowymi były akceptowane jako takie również w innych państwach członkowskich. Rozporządzenie nie powinno mieć wpływu na prawo państw członkowskich do stanowienia o tym, co stanowi oryginał lub odpis na poziomie krajowym, lecz powinno zapewnić możliwość stosowania ich jako takich również w kontekście transgranicznym.

Zagraniczny dokument urzędowy ma moc dowodową na równi z polskim dokumentem urzędowym (art. 1138 KPC)[6]. Można go zdefiniować jako dokument sporządzony przez organ państwa obcego w ramach powierzonych mu kompetencji we właściwej formie[7]. W wielu krajach dopuszczono możliwość sporządzania dokumentów urzędowych w postaci elektronicznej. Oznacza to, że powinny one być traktowane jako urzędowe również przed polskim sądem cywilnym.

Zagraniczne dokumenty prywatne na gruncie prawa procesowego mają walor krajowych dokumentów prywatnych. Bez przeszkód zatem można na gruncie obecnego prawa przed polskim sądem powoływać się na zagraniczne elektroniczne dokumenty prywatne. Pojawia się jednak problem z dostarczeniem takiego dokumentu do sądu. Praktycznie jest to możliwe tylko poprzez przesłanie elektronicznego nośnika informacji z zapisanym na nim dokumentem lub poświadczonym za zgodność na gruncie art.129 k.p.c. jego papierowym wydrukiem.

Projekt rozporządzenia bardziej szczegółowo reguluje problematykę identyfikacji elektronicznej niż dyrektywa 99/93/WE, która praktycznie odnosiła się głównie do podpisu elektronicznego, certyfikatu i nadzoru nad nimi. Projekt rozporządzenia, obok propozycji nowych narzędzi umożliwiających identyfikację elektroniczną, odnosi się także do kwestii dokumentów w postaci elektronicznej, uznawalności przekonwertowanych dokumentów tradycyjnych i uznawalności dokumentów w postaci elektronicznej w postępowaniach sądowych oraz przed organami publicznymi.

Rozporządzenie znajduje zastosowanie do usług identyfikacji elektronicznej świadczonych przez państwa członkowskie, w ich imieniu, na ich odpowiedzialność oraz w odniesieniu do dostawców usług zaufania posiadających siedzibę w Unii. Nie stosuje się go natomiast do świadczenia usług zaufania opierających się na dobrowolnych porozumieniach zawartych na mocy prawa prywatnego.

Projekt wprowadza definicję nowych pojęć oraz zawiera modyfikacje pojęć stosowanych na gruncie dyrektywy 99/93/WE.

Za „identyfikację elektroniczną" uznaje się proces używania danych identyfikujących osobę w formie elektronicznej, w sposób jednoznaczny reprezentujący osobę fizyczną lub prawną.

„Uwierzytelnianiem" jest proces elektroniczny, który umożliwia weryfikację identyfikacji elektronicznej osoby fizycznej lub prawnej lub pochodzenia i integralności danych elektronicznych.

Rozporządzenie kontynuuje zasadę, że podpisującym jest osoba fizyczna, która składa podpis elektroniczny. „Podpis elektroniczny" oznacza dane w formie elektronicznej dodane do innych danych elektronicznych lub logicznie z nimi powiązane i służące podpisującemu do składania podpisu. Należy zwrócić uwagę, iż w tej definicji zrezygnowano z dotychczasowego pojęcia „i służy do uwierzytelnienia" czy też jak w polskiej ustawie o podpisie elektronicznym do „identyfikacji". W nowym ujęciu podpis elektroniczny ma służyć do podpisywania. Kwestia uwie-

[5] COM(2012) 238. 2012/0146 (COD)

[6] Zob. także W. Broniewicz, Postępowanie cywilne w zarysie, Warszawa 1983, s. 181.

[7] T. Demendecki [w:] A. Jakubecki (red.), Kodeks postępowania cywilnego op. cit., s. 1389.

rzytelniania jak też identyfikacji pojawia się dopiero w definicji zaawansowanego podpisu elektronicznego będącego podpisem elektronicznym, który spełnia następujące wymagania: a) jest przyporządkowany wyłącznie podpisującemu; b) umożliwia ustalenie tożsamości podpisującego; c) jest składany przy użyciu danych służących do składania podpisu elektronicznego, które podpisujący może wykorzystać z dużą dozą zaufania i nad którymi ma wyłączną kontrolę; oraz d) jest w taki sposób powiązany z danymi, do których się odnosi, że każda późniejsza zmiana danych jest wykrywalna.

Szczególną postacią zaawansowanego podpisu elektronicznego jest „kwalifikowany podpis elektroniczny" będący zaawansowanym podpisem elektronicznym, który jest składany za pomocą urządzenia do składania kwalifikowanego podpisu elektronicznego i który opiera się na kwalifikowanym certyfikacie podpisu elektronicznego.

Definicje określone w projekcie rozporządzenia w sposób istotny zmienią sferę pojęciową w polskim prawie. Pojawi się nieznany w naszym systemie zaawansowany podpis elektroniczny, a w miejsce bezpiecznego podpisu elektronicznego weryfikowanego ważnym kwalifikowanym certyfikatem pojawi się kwalifikowany podpis elektroniczny. Zmiana ta jest o tyle istotna, iż w polskich przepisach nie zawsze wymagany jest bezpieczny podpis elektroniczny weryfikowany ważnym kwalifikowanym certyfikatem. Często ustawodawca z rozmysłem wymaga bezpiecznego podpisu elektronicznego, jednakże weryfikowanego zwykłym certyfikatem, czy nawet bez certyfikatu. Konieczna będzie weryfikacja przepisów odnoszących się do bezpiecznego podpisu elektronicznego i każdorazowe wskazanie, czy zastąpi go zaawansowany podpis elektroniczny, czy też bezpieczny podpis elektroniczny weryfikowany ważnym kwalifikowanym certyfikatem.

Całkowicie nowym, nieznanym dotychczas w polskim prawie, chociaż postulowanym w doktrynie[8] rozwiązaniem jest wprowadzenie pieczęci elektronicznej jako narzędzia będącego *de facto* odpowiednikiem podpisu elektronicznego ale pozwalającego na identyfikację innych podmiotów niż osoba fizyczna (której przyporządkowany jest wyłącznie podpis elektroniczny i jego kwalifikowane postaci).

W projekcie rozporządzenia „pieczęć elektroniczna" oznacza dane w postaci elektronicznej dodane do innych danych elektronicznych lub logicznie z nimi powiązane, aby zagwarantować pochodzenie i integralność powiązanych danych. Wprowadza się „zaawansowaną pieczęć elektroniczną" czyli pieczęć elektroniczna, która spełnia następujące wymagania a) jest przyporządkowana wyłącznie podmiotowi wystawiającemu pieczęć; b) umożliwia ustalenie tożsamości podmiotu wystawiającego pieczęć; c) jest tworzona przy użyciu danych służących do wystawiania pieczęci elektronicznej, które podmiot wystawiający pieczęć posiadający duży poziom zaufania może wykorzystać do wystawienia pieczęci elektronicznej; oraz jest w taki sposób powiązana z danymi, do których się odnosi, że każda późniejsza zmiana danych jest wykrywalna. Wreszcie proponuje się kwalifikowaną postać pieczęci, czyli „kwalifikowaną pieczęć elektroniczną" będącą zaawansowaną pieczęcią elektroniczną, która została wystawiona za pomocą urządzenia do wystawiania kwalifikowanych pieczęci elektronicznych i która opiera się na kwalifikowanym certyfikacie pieczęci elektronicznej;

Zgodnie z proponowanym art. 28 rozporządzenia nie można kwestionować prawnego skutku pieczęci elektronicznej ani jej dopuszczalności jako dowodu w postępowaniu sądowym wyłącznie z tego powodu, że ma postać elektroniczną.

Kwalifikowana pieczęć elektroniczna umożliwia prawne domniemanie pochodzenia i integralności danych, do których jest dołączona i jest uznawana i akceptowana we wszystkich państwach członkowskich. Gdy wymagana jest – w szczególności przez państwo członkowskie na potrzeby uzyskania dostępu do usługi publicznej oferowanej przez organ publiczny online, na podstawie odpowiedniej oceny ryzyka zawiązanego z taką usługą – pieczęć elektroniczna o poziomie bezpieczeństwa niższym niż kwalifikowana pieczęć elektroniczna, akceptowane są wszystkie pieczęci elektroniczne o co najmniej takim samym poziomie bezpieczeństwa. W przypadku transgranicznego dostępu do usługi oferowanej przez organ publiczny *online,* państwa członkowskie nie wymagają pieczęci elektronicznej o wyższym poziomie bezpieczeństwa niż kwalifikowana pieczęć elektroniczna.

Narzędzie pieczęci elektronicznej i jej kwalifikowane postaci jako nieznane polskiemu prawu, będą wymagały odpowiedniej zmiany przepisów oraz rozważań nad sposobem ich wykorzystania, tj. ustalenia do jakich czynności będą miały zastosowanie, a także ustalenia ich powiązania z teorią organów i kwestią reprezentacji[9] łącznej.

Podobne rozwiązanie, jak w przypadku pieczęci elektronicznej, znajdzie się w odniesieniu do podpisów elektronicznych. Zgodnie art. 20 rozporządzenia, nie można kwestionować prawnego skutku podpisu elektronicznego ani jego dopuszczalności jako dowodu w postępowaniu sądowym wyłącznie z tego powodu, że ma formę elektroniczną. Zbliżona regulacja zawarta jest już w art. 9 dyrektywy nr 2000/31/WE Parlamentu Europejskiego i Rady w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego[10] (dyrektywa o handlu elektronicznym). Zgodnie z tym przepisem Państwa Członkowskie zapewniają, żeby ich system prawny umożliwiał zawieranie umów drogą elektroniczną. Państwa Członkowskie są zobowiązane w szczególności o zadbanie, by wymagania prawne mające zastosowanie do procesu zawierania umów nie stanowiły przeszkody dla używania umów elektronicznych ani nie prowadziły do pozbawienia prawnej skuteczności i ważności takich umów z tego powodu, że są one zawierane drogą elektroniczną. Ustawy krajowe nie mogą ograniczać możliwości dowodzenia określonych faktów za pomocą dokumentów elektronicznych.

Kwalifikowany podpis elektroniczny ma skutek prawny równoważny ze skutkiem prawnym podpisu własnoręcznego. Kwalifikowane podpisy elektroniczne są uznawane i akceptowane we wszystkich państwach członkowskich. Natomiast, gdy wymagany będzie – w szczególności przez jedno państwo członkowskie na potrzeby uzyskania dostępu do usługi publicznej oferowanej przez organ publiczny online, na podstawie odpowiedniej oceny ryzyka zawiązanego z taką usługą – podpis elektroniczny o po-

[8] Por. J. Gołaczyński, D. Szostek: Czy pieczęć elektroniczna ma szanse usprawnić e-administrację, MoP 5/2009, str. 21 i nast.

[9] W polskiej literaturze na temat koncepcji pieczęci elektronicznej pisał J. Gołaczyński, Dariusz Szostek: Czy pieczęć elektroniczna ma szansę usprawnić e-administrację? , MoP 2009, Nr.5. str. 278 i nast.

[10] Dyrektywa nr 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8.6.2000r.

ziomie bezpieczeństwa niższym niż kwalifikowany podpis elektroniczny, akceptowane będą wszystkie podpisy elektroniczne, o co najmniej takim samym poziomie bezpieczeństwa. W przypadku transgranicznego dostępu do usługi oferowanej online przez organ publiczny, państwa członkowskie nie będą wymagały podpisu elektronicznego o wyższym poziomie bezpieczeństwa niż kwalifikowany podpis elektroniczny.

Dla polskiego wymiaru sprawiedliwości istotna jest natomiast propozycja art.34 projektowanego rozporządzenia. W aktualnym stanie prawnym nie ma możliwości, poza chlubnym wyjątkiem elektronicznego postępowania upominawczego, wnoszenia pism do sądu, ani doręczania stronom dokumentów w postaci elektronicznej. Po wejściu w życie rozporządzenia, wszystkie sądy będą musiały przyjmować wszelkiego typu pisma procesowe w postaci elektronicznej, a także przekonwertowane do tej postaci dokumenty papierowe. Warto podkreślić, że zaproponowana w rozporządzeniu definicja dokumentu elektronicznego, to jest dokumentu w dowolnym formacie elektronicznym, jest zbieżna z projektowaną definicją dokumentu, która znajdzie się w nowelizowanym Kodeksie cywilnym. Na uwagę zasługuje także wprowadzenie zasady zrównania pod względem skutków prawnych dokumentu elektronicznego i papierowego. Zgodnie z art.34 pkt.1 projektu rozporządzenia dokument elektroniczny uznaje się za równoważny dokumentowi papierowemu oraz dopuszczalny jako dowód w postepowaniu sądowym, z uwzględnieniem jego poziomu zabezpieczenia, autentyczności i integralności. Dokument zawierający kwalifikowany podpis elektroniczny lub kwalifikowana pieczęć elektroniczna osoby, która jest uprawniona do wydawania stosownych dokumentów, umożliwia prawne domniemanie autentyczności i integralności, pod warunkiem że dokument nie zawiera dynamicznych elementów, które mogą go automatycznie zmienić. Istotne jest także usankcjonowanie konwersji dokumentu tradycyjnego do postaci elektronicznej. W sytuacji, gdy do celu świadczenia usługi publicznej *online* oferowanej przez organ sektora publicznego wymagany jest oryginalny dokument lub uwierzytelniony odpis, przynajmniej dokumenty elektroniczne wydane przez osoby uprawnione do wydawania stosownych dokumentów i uznawane za oryginały lub uwierzytelnione odpisy zgodnie z przepisami krajowymi państwa członkowskiego pochodzenia, akceptuje się w pozostałych państwach członkowskich bez konieczności spełnienia dodatkowych wymogów. Wydaje się, że przepis ten jest spójny z projektem nowelizacji art.129 § 2 polskiego k.p.c., zgodnie z którym zamiast oryginału, strona może złożyć odpis dokumentu, jeżeli jego zgodność z oryginałem została poświadczona przez notariusza albo przez występującego w sprawie pełnomocnika strony będącego adwokatem, radcą prawnym, rzecznikiem patentowym lub radcą Prokuratorii Generalnej Skarbu Państwa. Elektroniczne poświadczenie odpisu dokumentu następuje z chwilą wprowadzenia tego dokumentu do systemu teleinformatycznego.

Uznanie poświadczonego w postaci elektronicznej dokumentu urzędowego za równoważny odpisowi, oznacza zrównanie ich mocy dowodowej z taką, jaka jest przypisana dokumentom w oryginale sporządzonym w tradycyjnej „papierowej" postaci. Poświadczony w postaci elektronicznej dokument urzędowy cechować się będzie również domniemaniem prawdziwości i zgodności z prawdą tego, co zostało w nim urzędowo zaświadczone.

Projekt omawianego rozporządzenia w istotny sposób zmieni reguły dotyczące identyfikacji elektronicznej podmiotów w transakcjach elektronicznych. Przede wszystkim wprowadzi nowe, ale jak się wydaje oczekiwane przez rynek, narzędzia. Rozporządzenie pozwala mieć nadzieję na rozwiązanie szeregu problemów podnoszonych dotychczas doktrynie, i to zarówno polskiej jak i zagranicznej w zakresie elektronicznej identyfikacji, wykorzystania dokumentów elektronicznych w postępowaniach, w tym sądowych, konwersji dokumentów do postaci elektronicznej itd. Dla rozporządzenia przyjęto 6 miesięczne vacatio legis i wiele wskazuje na to, że wejdzie ono w życie w 2014 roku. Należy dodać, że w trakcie procesu legislacyjnego w Parlamencie Europejskim wprowadzane są liczne poprawki (zgłoszono ich kilkaset), dlatego też ostateczne brzmienie przepisów rozporządzenia może w szczegółach różnić się od powyżej przedstawionej regulacji.

Abstract

Dariusz Szostek and Berenika Kaczmarek-Templin in the dissertation, "Electronic identification of entities in the Draft Regulation of the European Parliament ... „refer to the issue of identification of the services of confidence - electronic transactions on the internal market. Recognition of an electronically certified document to be equivalent to a copy, it means equating their probative value to such, which is assigned to documents in original, in the traditional „paper" form. Certified in an electronic form an official document will be characterized by the presumption of validity and veracity of what was in it officially attested. The draft of the discussed regulation will significantly change the rules on the electronic identification of entities in electronic transactions. First of all, it will introduce new tools expected by the market. The regulation brings hope to solve a number of issues raised previously by doctrine, both Polish and foreign electronic identification in the scope of the use of electronic documents in the proceedings, including judicial acts, conversion of documents into electronic form, etc. For the regulation was adopted a six year vacatio legis, and much indicates that it will come into force in 2020. It should be added that during the legislative process in the European Parliament, numerous amendments are introduced (several hundred reported) , and therefore the final wording of the provisions of Regulation may differ in detail from the above - presented adjustment.

AGATA JAROSZEK

DZIECKO JAKO PODMIOT OCHRONY PRAWNEJ W PROJEKCIE ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY W SPRAWIE OCHRONY OSÓB FIZYCZNYCH W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH I SWOBODNEGO PRZEPŁYWU TYCH DANYCH

Unijna reforma ochrony danych ma na celu stworzenie nowoczesnych, solidnych, spójnych i kompleksowych ram ochrony danych w Unii Europejskiej. Komisja proponuje, by nowe ramy prawne obejmowały dwa projekty (wnioski ustawodawcze) mianowicie: (zastępujący dyrektywę 95/46/WE)[1] wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (ogólne rozporządzenie o ochronie danych)[2], oraz – wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy na potrzeby zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania lub wykonywania kar kryminalnych oraz swobodnego przepływu takich danych[3]. W niniejszym opracowaniu uwaga zostanie poświęcona wyłącznie projektowi „ogólne rozporządzenie o ochronie danych".

Projekt rozporządzenia zakłada doprecyzowanie spornych czy niejasnych zapisów w dyrektywie jak również wprowadzenie nowych regulacji dzięki którym znacznemu wzmocnieniu uległyby prawa osób fizycznych do ochrony swoich danych oraz kontrola nad zarządzaniem oraz przetwarzaniem danych osobowych. Przede wszystkim proponuje się wzmocnienie prawa podstawowego osób fizycznych do ochrony danych oraz przestrzeganie innych praw, takie jak wolność wypowiedzi i informacji, prawa dziecka, prawo do prowadzenia działalności gospodarczej, prawo do rzetelnego procesu sądowego i obowiązek zachowania tajemnicy zawodowej (na przykład w zawodach prawniczych)[4].

Innowacyjność projektu przejawia się między innymi w następujących kwestiach: po pierwsze przedstawiono nowe definicje pojęć np. „dane genetyczne", „dane biometryczne", „wiążące reguły korporacyjne" czy definicję dziecka w oparciu o definicję Konwencji ONZ o prawach dziecka, po drugie sformułowano nowy katalog praw przysługujących podmiotowi danych tj. prawo do zmiany (poprawy) czy usunięcia danych, prawo do „bycia zapomnianym w środowisku cyfrowym", prawo sprzeciwu, prawo, że podmiot danych musi *być* poinformowany o *profilowaniu* i ma *prawo nie* wyrazić na *nie* zgody. Projekt również w jaśniej niż dotychczas formułuje warunki uzyskiwania zgody (w szczególności w sytuacjach przetwarzania danych dotyczących dzieci).

W zakresie obowiązków informacyjnych administratorów oraz podmiotów przetwarzających Komisja proponuje ich uszczegółowienie w następujących kwestiach: poinformowania podmiotów danych o naruszeniach, zachowania większej przejrzystości zasad przetwarzania danych czy wprowadzenia odpowiednich środków mających na celu zapewnienie bezpieczeństwa przetwarzania. Projekt ustanawia ogólne ramy sankcji (głównie administracyjnych), a także zapewnia w szerszym stopniu niż jak dotychczas regulowała to dyrektywa 95/46/WE środki ochrony prawnej.

W projekcie rozporządzenia po raz pierwszy wymieniono dziecko jako podmiot zasługujący na szczególną ochronę. Nie oznacza to, że wcześniej dzieci nie korzystały z ochrony prawnej w zakresie przetwarzania danych osobowych, gdyż zgodnie z przepisami dyrektywy 95/46/WE dzieciom jako osobom fizycznym przysługują takie same prawa jak dorosłym np. prawa do poprawienia, usunięcia lub zablokowania danych czy prawo do wyrażenia sprzeciwu. **Komisja widzi potrzebę wzmocnienia prawa do ochrony danych osobowych**. W tym celu proponuje

[1] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Dz.U. L 281 z 23.11.1995, s. 31

[2] Rozporządzenie to wprowadza również ograniczoną liczbę poprawek technicznych do dyrektywy w sprawie e-prywatności (dyrektywy 2002/58/WE ostatnio zmienionej dyrektywą 2009/136/WE – Dz.U. L 337 z 18.12.2009, s. 11) w celu uwzględnienia przekształcenia dyrektywy 95/46/WE w rozporządzenie. Te istotne skutki prawne wprowadzenia nowego rozporządzenia i nowej dyrektywy dla przepisów dyrektywy w sprawie e-prywatności będą w odpowiednim terminie przedmiotem przeglądu Komisji, z uwzględnieniem wyników negocjacji w sprawie bieżących propozycji z Parlamentem Europejskim i Radą. Zob. Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów Ochrona prywatności w połączonym świecie – europejskie ramy ochrony danych w XXI wieku /* COM/2012/09 final */ Komunikat zawiera opis najważniejszych elementów reformy unijnych ram ochrony danych.

[3] Dyrektywa zastępująca decyzja ramowa 2008/977/JHA z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych, Dz.U. L 350 z 30.12.2008, s. 60. Sprawozdanie dotyczące wdrażania przez państwa członkowskie decyzji ramowej (COM(2012) 12) jest przyjmowane jako element pakietu reformy ochrony danych. Zob. Wniosek Dyrektywa Parlamentu Europejskiego I Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych oraz swobodnego przepływu tych danych /* COM/2012/010 final - 2012/0010 (COD) */

[4] Komunikat Komisji Do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów Ochrona prywatności w połączonym świecie – europejskie ramy ochrony danych w XXI wieku /* COM/2012/09 final */ Komunikat zawiera opis najważniejszych elementów reformy unijnych ram ochrony danych

wprowadzenie nowych regulacji (przepisów), które zwiększą osobom fizycznym możliwości kontroli swoich danych. W szczególności należy na podstawie nowych przepisów wzmocnić prawa do bycia poinformowanym, tak aby osoby fizyczne w pełni rozumiały, w jaki sposób ich dane osobowe są przetwarzane, w szczególności gdy przetwarzanie to dotyczy dzieci[5].

Punktem wyjścia dla zapewnienia dzieciom szczególnej ochrony prawnej w zakresie danych osobowych w projekcie rozporządzenia jest przyjęcie założenia, że *„dzieci mogą być w mniejszym stopniu świadome zagrożeń, konsekwencji, gwarancji i praw w związku z przetwarzaniem danych osobowych"* (co znalazło wyraz w proponowanym przez Komisję brzmieniu preambuły 29)[6].

W stosunku do dyrektywy 1995/46/WE projekt rozporządzenia wprowadza nową definicję dziecka w art. 4.18 zgodnie z którą dziecko to każda osoba poniżej 18-go roku życia. Projektowana definicja nawiązuje do konwencyjnej definicji dziecka w Konwencji ONZ o prawach dziecka[7]. W rozumieniu artykułu 1 konwencji „dziecko" oznacza każdą istotę ludzką w wieku poniżej osiemnastu lat, chyba że zgodnie z prawem odnoszącym się do dziecka uzyska ono wcześniej pełnoletność. Każde państwo – strona Konwencji indywidualnie rozstrzyga, jaki zakres ochrony jest właściwy dla określonego etapu rozwoju dziecka. Konwencja nie wprowadza żadnych innych ograniczeń podmiotowych poza wyodrębnieniem granic wiekowych dziecka (0–18 lat)[8]. Górna granica dzieciństwa jest określona jako wiek dziecka niż jako pełnoletniość uznając, że w większości systemów prawnych dziecko może nabyć pełną zdolność do czynności prawnych w zakresie różnych czynności w różnym wieku[9].

Preambuła Konwencji ONZ powołuje się Deklarację Praw Dziecka, w której wskazano, że „dziecko, z uwagi na swoją niedojrzałość fizyczną oraz umysłową, wymaga szczególnej opieki i troski, w tym właściwej ochrony prawnej, zarówno przed, jak i po urodzeniu". Można więc uznać, że definicja przyjęta w art. 1 Konwencji ONZ wyznacza pewien minimalny standard w związku z art. 41 zgodnie z którym niniejsza konwencja w żaden sposób nie narusza postanowień, które w większym stopniu sprzyjają realizacji praw dziecka i które mogą być zawarte w: a) prawie Państwa-Strony lub b) prawie międzynarodowym obowiązującym to Państwo, to jednak nie istnieje synchronizacja na poziomie międzynarodowym odnośnie ustalenia górnej granicy wiekowej wyznaczający okres bycia/pozostawania dzieckiem. Co więcej art. 16 Konwencji ONZ o prawach dziecka stwierdza, że 1. Żadne dziecko nie będzie podlegało arbitralnej lub bezprawnej ingerencji w sferę jego życia prywatnego, rodzinnego lub domowego czy w korespondencję ani bezprawnym zamachom na jego honor i reputację. 2. Dziecko ma prawo do ochrony prawnej przeciwko tego rodzaju ingerencji lub zamachom.

Obok nowej definicji dziecka (art. 4.18) w art. 8 Komisja określa dodatkowe warunki zapewnienia zgodności prawem przetwarzania danych osobowych dzieci w odniesieniu do usług społeczeństwa informacyjnego oferowanych im bezpośrednio, który jest nowym przepisem w stosunku do dyrektywy 95/45/WE. Inicjatywa Komisji podjęta w tym zakresie jest właściwa ze względu na coraz większą aktywność dzieci online, (np. gry online), uczestnictwo na portalach społecznościowych, gdzie dzieci powinny być świadome z kim się komunikują, a także ze względu działalność marketingową, której adresatami są dzieci.

Wśród przedstawionych opinii na temat projektu Komisji wyrażonych przez zainteresowane podmioty, w tym przedstawicieli Parlamentu Europejskiego podkreśla się, że wszędzie tam gdzie przepisy wyraźnie odnoszą się do zagwarantowania ochrony prawnej dziecku, nie należy interpretować, że na gruncie rozporządzenia osoby pełnoletnie są mniej chronione[10]. Nie budzi wątpliwości sama idea objęcia szczególną ochroną dzieci w przypadku przetwarzania ich danych w oparciu o zgodę, gdyż wychodzi się ze słusznego założenia, że dzieci często nie są świadome niebezpieczeństwa, bądź ryzyka, które jest związane z faktem korzystania z usług oferowanych *online* (w internecie). Po pierwsze co do zasady dzieci w mniejszym stopniu niż dorośli posiadają umiejętność krytycznej oceny przekazywanych im informacji przez przedsiębiorców (bądź te umiejętności są niewystarczające do właściwej oceny skutków wyrażenia zgody na korzystanie z oferty danego serwisu). Analogicznie dzieci nie rozumieją (bądź nie do końca zdają sobie sprawę) jakie skutki może wywoływać w sferze prywatności stosowane metody i praktyki przez reklamodawców (dotyczy to przede wszystkim właściwej oceny potencjalnych skutków wykorzystywania reklamy behawioralnej oraz innych praktyk reklamowych mający natarczywy charakter)[11].

Powszechną praktyką serwisów oferujących np. aplikacje mobilne, darmowe gry jest zbieranie danych od dzieci (np. imię nazwisko, wiek, nr telefonu lub adres poczty elektronicznej w celach marketingowych). Nawet jeżeli dziecko nie chce ujawnić swoich danych, często uzyskanie dostępu do innych poziomów gry (np. wydłużenie czasu gry, zakup nowego życia czy dodatkowych punktów pozwalających na kontynuowania gry) lub możliwość „darmowego" korzystania z innych funkcji programów jest uzależnione właśnie od przekazania operatorowi dodatkowych informacji na swój temat. Po drugie jak również pokazuje to praktyka wyrażenie poinformowanej zgody przez dziecko czy osobę nastoletnią jest uzależnione od zaakceptowania warunków serwisu, które w praktyce często przyjmują formę wielostronicowego tekstu, napisanego skomplikowanym językiem prawniczym, małą czcionką, co znacznie utrudnia lekturę takiego tekstu. Dlatego należy uznać za całkiem uzasadnione twierdzenie, że nie jest możliwe, aby dzieci faktycznie zapoznały się z treścią takiej

[5] Komunikat Komisji Do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów Ochrona prywatności w połączonym świecie – europejskie ramy ochrony danych w XXI wieku /* COM/2012/09 final */

[6] Wniosek Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) COM(2012) 11 final

[7] Konwencja ONZ o prawach dziecka (Dz.U. z 1991 r. Nr 120, poz. 526).Aby stwierdzić, czy dana osoba jest dzieckiem, w niniejszym rozporządzeniu należy przyjąć definicję określoną w Konwencji Narodów Zjednoczonych o prawach dziecka. Por. preambuła 29 zd. 2. projektu rozporządzenia.

[8] W tym dziecka nienarodzonego, a zatem czy będzie mu przysługiwało prawo do życia i przeżycia w: J. Brzezińska, Dzieciobójstwo. Aspekty prawne i etyczne, przypis 66. Polskie ustawodawstwo określa ogólną granicę pełnoletności na 18 lat, aczkolwiek w innych krajach w pewnych szczególnych sytuacjach górna granica pełnoletniości jest określona na 21 lat np. w Indiach, Stanach Zjednoczonych.

[9] India: First Periodic Report on the CRC. Published by the Department of Women and Child Development,. Ministry of Human Resource Development.

[10] Opinion of the Committee on Industry, Research and Energy for the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

[11] Komisja powołała się na badanie, którego jasno wynika, że dzieci w wieku 9-10 oraz 12- 14 lat zazwyczaj nie doceniają zagrożeń związanych z wykorzystaniem Internetu i bagatelizują konsekwencje swoich ryzykownych zachowań Zob. jakościowe badanie „Bezpieczniejszy Internet dla dzieci" dotyczące dzieci w wieku 9-10 oraz 12- 14 lat, które pokazało, (dostępne na stronie: http://ec.europa.eu/information_society/activities/sip/surveys/qualitative/index_en.htm).

polityki prywatności czy z warunkami korzystania z serwisu, a przede wszystkie uznać, że dziecko rzeczywiście wie na co się zgadza, chcąc korzystać z usług danego portalu[12]. Ten argument jest szczególnie istotny w handlu mobilnym (ang. m-commerce), w przypadku korzystania z aplikacji mobilnych przez dzieci i młodzież, gdzie często nie jest możliwe wyświetlenie warunków korzystania z serwisów ze względu na mały rozmiar ekranu czy inne uwarunkowania (np. zbyt wolny transfer danych).

Przechodząc to analizy treści projektowanego przepisu art. 8 (*Przetwarzanie danych osobowych dziecka*) Komisja proponuje ustanowienie dodatkowych warunków legalności przetwarzania danych osobowych dzieci w związku usługami społeczeństwa informacyjnego. I tak zgodnie z proponowaną treścią: *art. 8 ust. 1 Do celów niniejszego rozporządzenia, w odniesieniu do oferowania usług społeczeństwa informacyjnego bezpośrednio dziecku, przetwarzanie danych osobowych dziecka w wieku poniżej 13 lat jest zgodne z prawem, o ile zgodę na nie wydał lub pozwolił na nie rodzic lub opiekun dziecka. Administrator podejmuje racjonalne starania w celu uzyskania możliwej do zweryfikowania zgody, uwzględniając dostępną technologię.*

Warto przedstawić opinie oraz uwagi co treści przedstawione przez zainteresowane podmioty. Rząd Wielkiej Brytanii stoi na stanowisku, że dziecko ma prawo dokonywać czynności prawnych w drobnych sprawach życia codziennego, których wartość ekonomiczna jest niewielka. Na przykład dzieci poniżej 13-go roku życia powinny mieć możliwość subskrypcji newslettera (pod postacią przesyłanych wiadomości poczty elektronicznej) swojego ulubionego zespołu, piosenkarza lub mieć możliwość skorzystania z pomocy psychologa przez Internet lub zgłosić przypadek przemocy stosowanej wobec niego bez interwencji ze strony dorosłych[13].

Nawiązując do opinii wydanej przez Rząd Brytyjski Committee on Legal Affairs Parlamentu Europejskiego proponuje nowy przepis (dodany jako kolejny ust. art. 8), który będzie miał zastosowanie do sytuacji, gdy przetwarzanie dotyczy danych na temat zdrowia dziecka oraz wtedy gdy, prawo państwa członkowskiego w zakresie opieki zdrowotnej i społecznej ustanowi priorytet kompetencji jednostki/osoby w stosunku do jej wieku biologicznego. Uzasadnieniem propozycji przepisu jest fakt, że w takich przypadkach weryfikacja/potwierdzenie rodzica lub opiekuna prawnego nie powinno być konieczne jeżeli dziecko ma kompetencje do podjęcia decyzji samodzielnie. Chodzić tutaj może o możliwość korzystania z konsultacji medycznych czy korzystania z porad psychologa (np. niebieskiej linii itp.)[14]

W opinii EDRI od rodziców lub opiekunów prawnych należy wymagać udzielenia/autoryzowania zgody na przetwarzanie danych dzieci, które nie ukończyły 13-go roku życia. Z kolei jeżeli chodzi o zakres przedmiotowy proponuje się, aby ten szczególny przepis miał zastosowanie do wszystkich towarów bądź usług oferowanych bezpośrednio dziecku, a nie wyłącznie do usług społeczeństwa informacyjnego[15]. W celu ustalenia wieku dziecka administratorzy danych nie powinni wykorzystywać metod umożliwiających zbieranie większej ilości danych wyłącznie w celu ustalenia wieku dziecka. Natomiast forma informacji na temat przetwarzania danych kierowana do dzieci powinna być sformułowana w języku dostosowanym do wieku dziecka, umożliwiającym mu zrozumienie operacji przetwarzania, a w konsekwencji wyrażenia świadomej zgody[16].

Jak zauważono w literaturze *„prawną ochronę dzieci komplikuje fakt, że dzieci nie mają tych samych zdolności poznawczych co osoby dorosłe, przez co nie mogą one w pełni dokonywać świadomych i samodzielnych wyborów, biorąc za nie odpowiedzialność"*[17]. W zależności od etapu jego rozwoju ochrona prawna powinna być dostosowana do szczególnej wrażliwości, potrzeb oraz zmienności zdolności poznawczych, które ewoluują wraz przechodzeniem przez kolejne etapy dojrzewania, które ostatecznie prowadzą do osiągnięcia dorosłości. Bezspornym argumentem dla właściwej identyfikacji podmiotów uprawnionych jest wiek, albowiem ten wpływa na ocenę pełnoletności danej osoby. Jednak osiągnięcie pełnoletności nie jest wbrew pozorom kryterium niezawodnym dla regulacji każdego rodzaju stosunków społecznych, gdzie podmiotem jest dziecko, szczególnie jest widoczne w kwestii ochrony danych osobowych i prywatności[18].

Kwestia uzasadnienia przyznania prawa do udzielenia ważnej zgody przez dziecko na przetwarzanie danych dotyczących jego osoby jest niezwykle złożona. W przepisach państw członkowskich implementujących przepisy dyrektywy 95/46/WE nie mamy wyraźnego unormowania kwestii uzyskania zgody od dzieci czy wskazania wieku uprawniającego do wykonywania swoich praw w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych. Niewątpliwie kwestię tą pozostawiono mechanizmom samoregulacji np. w postaci wydawanych wskazówek i zaleceń przez krajowe ograny ochrony danych osobowych czy kodeksów dobrych praktyk. Brytyjski organ ochrony danych osobowych w notatce na temat zbierania danych przez strony internetowe zaleca, aby w sytuacji, gdy strona internetowa prosi o dane osobowe dziecka, uzyskać zgodę rodzica lub opiekuna prawnego, chyba, że można rozsądnie dać wiarę, że dziecko dokładnie rozumie sytuację i jest w stanie podjąć świadomą decyzję. W Wielkiej Brytanii nie istnieje legalna definicja dziecka oparta na kryterium wieku co jest uzasadnione twierdzeniem, że dzieci w tym samym wieku mogą wykazywać zróżnicowany poziom dojrzałości i rozumowania, co wpływa na zdolność do podejmowania świadomych decyzji. Wymaga się uzyskania jakiejś formy zgody rodzica w celach przetwarzania danych dziecka poniżej 12-go roku życia oraz w przypadku, gdy wzrasta poziom ryzyka. Ocena czy zgoda jest wymagana zależy do już od konkretnego przypadku[19].

Natomiast w USA kwestia uzyskania zgody na przetwarzanie danych dziecka jest określona w *The Children's Online Privacy*

[12] Opinion on consumers and vulnerability. European Consumer Consultative Group

[13] Proposed new EU General Data Protection Regulation: Article-by-article analysis paper-http://www.ico.org.uk/news/~/media/documents/library/Data_Protection/Research_and_reports/ico_proposed_dp_regulation_analysis_paper_20130212_pdf.ashx.

[14] Opinion of the Committee on Legal Affairs for the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

[15] European Digital Rights (EDRI) Position on the Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Podobnie wypowiada się na ten temat Grupa Robocza Art. 29 w sprawie zmian unijnych przepisów, Opinia 01/2012 o projektach reformy ochrony danych.

[16] Opinion of the Committee on Legal Affairs for the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Zob. także Opinion of the Committee on the Internal Market and Consumer Protection for the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

[17] Prawa dziecka. red. A. Wróbel / Majkowska-Szulc/Tomaszewska, komentarz do art. 24

[18] Ibidem.

[19] Personal information online code of practice Information Commissioner Office.

Protection Act of 1998 (w skrócie COPPA). Przepisy COPPA nakładają obowiązki na operatorów stron internetowych, którzy oferują swoje produkty lub usługi dzieciom poniżej 13-go roku życia lub świadomie zbierają czy w inny sposób przetwarzają dane osobowe dzieci poniżej 13-go roku życia, nawet w przypadkach, gdy usługi nie są oferowane bezpośrednio dzieciom. W celu przetwarzania danych dzieci COPPA nakłada na operatorów obowiązek zyskania uprzedniej zgody rodzica możliwej do zweryfikowania (ang. *verified consent*) (np. poprzez wysłanie wiadomości z adresu poczty elektronicznej rodzica, podanego podczas procesu rejestracji, podanie danych karty kredytowej, złożenie zgody na piśmie czy przez telefon). Interesującym jest fakt za pomocą jakich kryteriów następuje kwalifikacja strony jako oferująca (kierująca) swoją działalność do dzieci. Federalna Komisja Handlu bierze pod uwagę następujące kryteria: tematyka, język, reklamy, inne cechy i funkcje np. występowanie postaci rysunkowe prezentacja graficzna, animacja oraz sposób przekazu treści dostosowany do określonych grup wiekowych.

Z kolei prawo hiszpańskie dotyczące ochrony danych osobowych wyraźnie stanowi, że dane osobowe osób powyżej 14-go roku życia mogą być przetwarzane za ich zgodą z wyjątkiem sytuacji, gdzie prawo wymaga, aby rodzice albo opiekunowie prawni uczestniczyli w dostarczeniu takich danych. Podobną interpretację przyjmuje portugalski organ ochrony danych osobowych, zgodnie z którą dzieci powyżej 14-go roku życia mogą wyrazić zgodę, w drobnych sprawach życia codziennego w wieku 12 lat, jednak istnieje ogólny wymóg konsultacji z rodzicem. W Niemczech lekarze, pracownicy socjalni, nauczyciele mają obowiązek dopełnienia należytej staranności w przypadku oceny zgody dzieci, które ukończyły 12 lat. W praktyce oznacza to, że *a priori* uznaje się taką zgodę udzieloną przez dziecko za ważną, ale to na administratorze spoczywa obowiązek właściwej oceny i konsultacji z rodzicami, a nawet obowiązek odmowy przyjęcia oświadczenia, w którym dziecko wyraziło zgodę, wszędzie tam gdzie jest to odpowiednie i uzasadnione okolicznościami sprawy. Francuski organ ochrony danych osobowych wyraźnie opowiedział się za obowiązkiem udzielenia przez rodzica pisemnej zgody na przetwarzanie danych przez szkołę. W Danii co do zasady granicą wieku jest 15 lat, w Szwecji 14-15, wyjątkowo 13, uwzględniając wszystkie elementy istotne dla oceny stanu faktycznego, w tym poziom dojrzałości dziecka. *The European NGO Alliance for Child Safety Online* (eNacso) wydał opinię, że zgoda rodzica jest wymagana zawsze w sytuacjach, kiedy nie można oczekiwać, że dziecko zrozumie na czym polega operacja przetwarzania danych jak również, że sam fakt uiszczenia zapłaty bądź zawarcia umowy na korzystanie z serwisu przez rodzica nie powinno być podstawą uznania przez właściciela serwisu, że w ten sposób została udzielona zgoda na przetwarzanie[20].

W polskim porządku prawnym udzielenie zgody na przetwarzanie danych osobowych jest czynnością prawną. Zgodnie z regulacją kodeksową dziecko do ukończenia 13 roku życia nie posiada zdolności do czynności prawnych, natomiast dziecko w wieku 13–18 lat posiada jedynie ograniczoną zdolność do czynności prawnych. Oznacza to, że dziecko co do zasady nie może samodzielnie udzielić zgody na przetwarzanie danych osobowych czy wizerunku. Rodzic (bądź opiekun prawny) jest zobowiązany wyrazić taką zgodę za dziecko. W przypadku dzieci powyżej 13 roku życia – konieczna jest dodatkowa zgoda rodzica (opiekuna prawnego) na zgodę wyrażoną przez dziecko[21]. Przyjęcie takiej konstrukcji przepisu określenia braku zdolności na gruncie kodeksu cywilnego (art. 12) oznacza, że pozbawienie zdolności do czynności prawnych małoletnich, którzy nie ukończyli jeszcze trzynastu lat, oraz całkowicie ubezwłasnowolnionych wynika z przyjęcia przez polskiego prawodawcę trafnego – generalnie – założenia, że osoby te nie są obiektywnie w stanie dokonywać czynności prawnych z dostatecznym rozeznaniem. Jednocześnie wysunięto argument następujący argument, z którym należy się zgodzić, że „należy rozważać zasadność ewentualnego obniżenia granicy wieku osób, których powinno w przyszłości dotyczyć pozbawienie zdolności do czynności prawnych wobec obserwowanego, coraz szybszego tempa rozwoju młodych pokoleń[22].

Niewątpliwie kwestia harmonizacji limitu wieku w takim instrumencie jakim jest rozporządzenie jest ograniczona przede wszystkim ze względu na sytuacje faktyczne mające charakter czysto wewnętrzny, gdzie obowiązuje prawo określonego państwa członkowskiego. W projekcie rozporządzenia przyjęto za tym, że od chwili niemowlęctwa do ukończenia 13-go roku życia dziecko nie może bez zgody rodzica bądź opiekuna prawnego samodzielnie decydować o przetwarzaniu danych, które dotyczą jego osoby. Pozostaje pytanie jak powinna wyglądać kwestia ważności zgody na przetwarzanie dzieci pomiędzy 14 a 18 rokiem życia? Czy na podstawie proponowanego zapisu art. 8 ust. 1 należy uznać, że dzieci, które ukończyły 13 lat mogą samodzielnie udzielać zgody na przetwarzanie danych osobowych[23]?

Częściowej odpowiedzi na postawione powyżej pytania można szukać w dalszych ustępach art. 8 projektu rozporządzenia, gdyż kolejny zapis przyznaje uprawnienie Komisji do wydawania aktów delegowanych zgodnie z art. 86 projektu w celu doprecyzowania kryteriów oraz wymogów dotyczących sposobów uzyskania zgody, podlegającej weryfikacji. Zgodnie z proponowaną treścią art. 8 ust. 3 – *w celu doprecyzowania kryteriów i wymogów dotyczących sposobów uzyskania możliwej do zweryfikowania zgody, o której mowa w ust. 1. W tym celu Komisja rozważa szczególne środki dla mikroprzedsiębiorców oraz małych i średnich przedsiębiorców*.

W opinii Grupy Roboczej Art. 29 nie jest konieczna regulacja kryteriów oraz wymogów dotyczących sposobów uzyskania zgody w sztywny sposób w formie wiążącego instrumentu UE, jak również dopuszczenie uregulowania tej kwestii w prawie krajowym. W konsekwencji mogłoby to doprowadzić do różnic między obowiązkami nałożonymi na administratorów danych, co byłoby sprzeczne z celem polegającym na zapewnieniu harmonizacji i stworzeniu równych warunków działania oraz nie zapewniłoby wymaganej elastyczności. Dlatego w celu usunięcia wątpliwości interpretacyjnych Grupa Robocza proponuje, aby w przyszłości

[20] Privacy Protection for Minors…? Wpis na blogu dostępny pod adresem: http://jefausloos.wordpress.com/2013/02/13/privacy-protection-for-minors/

[21] Regulacje dotyczące zagrożeń w Internecie. Fundacja Dzieci Niczyje, tekst dostępny pod adresem: http://fdn.pl/regulacje-dot-zagrozen-w-internecie. Zob. także uwagi do art. 23 na temat zgody, P. Barta, P. Litwiński, Ustawa o ochronie danych osobowych. Komentarz, 2 wydanie, C.H. Beck 2013 oraz cytowana tamże literatura.

[22] E. Gniewek, P. Machnikowski (red.), Kodeks cywilny. Komentarz. Wyd. 5, Warszawa 2013. komentarz do art. 12

[23] Takie stanowisko prezentuje Europejski Inspektor Ochrony Danych Osobowych Zob. Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - „European Strategy for a Better Internet for Children"

podjęto próby połączenia różnych metod opracowania kryteriów i wymogów wykształconych w praktyce, co może odbywać się już na poziome krajowym z zaangażowaniem się krajowych organów ochrony danych osobowych, a także mocy wskazówek lub zaleceń wydawanych przez Europejską Radę Ochrony Danych[24].

Jeżeli chodzi o szczególne traktowanie mikroprzedsiębiorców oraz małych i średnich przedsiębiorców zarówno Grupa Robocza oraz EDRI wyraziło pewne zastrzeżenia co proponowanego wyłączenia MŚPz obowiązku uzyskiwania zgody jeżeli chodzi o przetwarzanie danych dzieci, gdyż jak słusznie zauważa EDRI rozmiar (np. liczba zatrudnionych pracowników) przedsiębiorstwa prowadzącego działalność w szczególności w Internecie nie musi oznaczać, że takie przedsiębiorstwo osiąga mniejsze zyski np. Instagram, który zatrudnia 10 osób wyceniono na ponad miliard dolarów[25].

Podsumowując analizę szczególnego przepisu odnoszącego się do przetwarzania danych dziecka w art. 8 projektu rozporządzenia, warto zwrócić uwagę na pozostałe przepisy, których celem jest spełnienie wymogu zapewnienia szczególnej ochrony dziecka. Nawiązując do sformułowania, że „dzieci mogą być w mniejszym stopniu świadome zagrożeń, konsekwencji, gwarancji i praw w związku z przetwarzaniem danych osobowych" (preambuła 29)[26]. Zgodnie z art. 6 ust. 1 lit. f) słuszny interes może stanowić podstawę prawną przetwarzania danych osobowych, o ile – i w zakresie, w jakim – spełniono określone warunki dotyczące wymogu przeprowadzenia testu równowagi w świetle okoliczności każdego przypadku. W przypadku przetwarzania danych osobowych, jeżeli jest ono konieczne dla celów wynikających ze słusznych interesów realizowanych przez administratora w opinii Komisji należałoby dokonać rzetelnej oceny, czy w sytuacji, gdy podmiotem danych jest dziecko, interesy lub podstawowe prawa i wolności dotyczące jego danych nie mają charakteru nadrzędnego (preambuła 38 w powiązaniu z art. 6 ust. 1 lit. f), co w konsekwencji może prowadzić do uznania przetwarzania danych realizowanego na podstawie słusznego interesu administracyjnego za bezprawne[27].

W przypadku spełniania obowiązków informacyjnych spoczywających na administratorze danych wymóg zapewnienia szczególnej ochrony dziecku wynika z zasady przejrzystości zgodnie z którą wszelkie informacje i komunikaty adresowane do dziecka, również na temat czy dane dotyczące dziecka są zbierane, w jakim celu i przez kogo powinny być formułowane w jasnym i prostym języku, zrozumiałym dla dziecka. Dotyczy to w szczególności takich sytuacji jak np. reklama w internecie, w których duża liczba podmiotów i złożoność technologiczna (w tym specyfika komunikacji na odległość) utrudnia podmiotowi danych uzyskanie rzetelnej informacji na temat przetwarzaniu jego danych (preambuła 46 w powiązaniu z art. 11 ust. 2)

Po trzecie w projekcie Komisja podkreśla też prawo dziecka do poprawienia jego danych osobowych oraz „prawo do bycia zapomnianym", jeśli przechowywanie tych danych nie jest zgodne z rozporządzeniem. W szczególności podmioty danych powinny mieć prawo do tego, by ich dane osobowe zostały usunięte i nie były dalej przetwarzane, jeśli dane te nie są już konieczne do celów, dla których dane są zbierane lub przetwarzane w inny sposób, jeśli podmioty danych odwołały zgodę na przetwarzanie lub jeśli wnoszą sprzeciw wobec przetwarzania danych osobowych ich dotyczących, lub jeśli przetwarzanie ich danych osobowych nie jest zgodne z niniejszym rozporządzeniem z innego powodu. Prawo to ma szczególne znaczenie wtedy, gdy podmiot danych wyraził zgodę jako dziecko, nie będąc w pełni świadomy ryzyk związanych z przetwarzaniem, a w późniejszym czasie chce usunąć takie dane osobowe, zwłaszcza z internetu[28] (preambuła 57 w powiązaniu z art. 17 projektu). Wydaje się być słuszną uwaga, że należy zaznaczyć, że to „prawo do bycia zapomnianym" powinno dotyczyć zarówno osoby pełnoletniej jak i dziecka, które ciągle pozostaje dzieckiem.

Kolejnym zapisem w projekcie, którego bezpośrednim adresatem jest dziecko jest prawo podmiotu danych do informacji o profilowaniu i związane z tym uprawnienie, polegające na tym, że podmiot danych ma prawo nie wyrazić na nie zgody. Zgodnie z propozycją Komisji profilowanie może być dozwolone wtedy, gdy jest wyraźnie przewidziane przez przepisy prawa, stosowane w toku zawierania lub wykonywania umowy lub gdy podmiot danych wyraził na niego zgodę, nie powinno ono dotyczyć dzieci. (preambuła 58 w powiązaniu z art. 20 projektu)

W art. 33 projektu, który wprowadza obowiązek przeprowadzania przez administratorów i podmioty przetwarzające oceny skutków w zakresie ochrony danych przed podjęciem ryzykownych operacji przetwarzania podkreślono, że przetwarzanie danych osobowych w wielkoskalowych zbiorach danych dotyczących dzieci, danych genetycznych lub biometrycznych stanowi szczególne ryzyko, w związku z tym jeśli operacje przetwarzania stwarzają szczególne ryzyko dla praw i wolności podmiotów danych z racji swego charakteru, zakresu lub celów, administrator lub podmiot przetwarzający przeprowadzają w imieniu administratora danych ocenę skutków przewidywanych operacji przetwarzania w zakresie ochrony danych osobowych (art. 33 ust. 1 oraz art. 33 ust. 2 lit. d).

[24] Zob. Grupa Robocza Art. 29, Opinia 08/2012 przedstawiająca dalsze uwagi dotyczące dyskusji na temat reformy ochrony danych oraz Working Document 01/2013 Input on the proposed implementing acts (WP 200). Komisja proponuje nadanie Grupie Roboczej Art. 29 statusu niezależnej Europejskiej Rady Ochrony Danych, aby zwiększyć jej wkład w spójne stosowanie przepisów o ochronie danych i stworzyć solidną podstawę do współpracy organów ochrony danych, w tym Europejskiego Inspektora Ochrony Danych. Zob. Ochrona prywatności w połączonym świecie – europejskie ramy ochrony danych w XXI wieku

[25] Grupa Robocza Art. 29 Opinia 08/2012 przedstawiająca dalsze uwagi dotyczące dyskusji na temat reformy ochrony danych. Zob. także European Digital Rights (EDRI) Position on the Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

[26] Wniosek Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) COM(2012) 11 final

[27] W projekcie rozporządzenia Komisja zastrzega sobie uprawnienie w przypadku przetwarzania danych osobowych dotyczących dziecka w szczególności do przyjmowania aktów delegowanych zgodnie z art. 86 w celu doprecyzowania warunków, o których mowa w art. 6 ust. 1 lit. f), dla różnych sektorów i sytuacji, w których przetwarza się dane. Art. 29 Grupa Robocza wyraża wątpliwość czy akt delegowany byłby właściwym instrumentem do uregulowania tego zasadniczego elementu rozporządzenia i czy pozostawienie dalszych regulacji w gestii ustawodawcy krajowego nie doprowadziłoby do wysoce niepożądanych różnic w wykładni i stosowaniu. Administratorzy danych mogliby wówczas przetwarzać dane na tej podstawie w jednym państwie członkowskim, a w innym potencjalnie nie. Dlatego też, aby zapewnić spójną interpretację i stosowanie niniejszej podstawy prawnej przetwarzania danych, należy przedstawić wytyczne na szczeblu europejskim. Wydaje się, że zamiast uregulować tę kwestię w akcie delegowanym właściwszym rozwiązaniem zapewniającym niezbędną elastyczność będą wskazówki wydawane przez EROD dotyczące tego, w jakich okolicznościach można powoływać się na „słuszny interes" oraz w jaki sposób ocenić, czy nadrzędny charakter w stosunku do takiego interesu mają interesy lub podstawowe prawa i wolności podmiotu danych, między innymi poprzez podanie konkretnych przykładów. Opinia 08/2012 przedstawia dalsze uwagi dotyczące dyskusji na temat reformy ochrony danych.

[28] Komisja proponuje, aby prawo do poprawy i usunięcia danych nie dotyczyło sytuacji, gdy dalsze przechowywanie jest niezbędne do celów dokumentacji, statystyki i badań naukowych, realizacji interesu publicznego w dziedzinie zdrowia publicznego, wykonania prawa wolności wypowiedzi, jeśli wymagają tego przepisy prawa lub jeśli są powody ograniczenia przetwarzania danych zamiast ich usunięcia.

Art. 38 projektu dotyczy kodeksów postępowania[29], wyjaśnia treść tych kodeksów i procedur oraz przewiduje uprawnienie Komisji do podejmowania decyzji w sprawie ogólnego obowiązywania kodeksów postępowania. Zgodnie z art. 38 ust. 1 lit. e) Państwa członkowskie, organy nadzorcze i Komisja zachęcają do sporządzania kodeksów postępowania, które mają przyczynić się do właściwego stosowania niniejszego rozporządzenia, z uwzględnieniem szczególnych cech różnych sektorów, w których odbywa się przetwarzanie, w szczególności w zakresie: informowania i ochrony dzieci. Natomiast art. 52 określa obowiązki organu nadzorczego, w tym dotyczące rozpatrywania skarg i prowadzenia postępowań w ich sprawie oraz szerzenia w społeczeństwie wiedzy na temat ryzyka, przepisów, gwarancji i praw. Komisja zobowiązuje każdy organ nadzorczy do działania na rzecz pogłębiania w społeczeństwie świadomości w zakresie ryzyka, przepisów, gwarancji oraz praw związanych z przetwarzaniem danych osobowych. Szczególną uwagę zwraca się na działania skierowane do dzieci.

Obecnie projekt poddany został wielostronnym konsultacjom, jak dotychczas zgłoszono ok. 4000 tys. poprawek, które również dotyczą przepisów regulujących prawa i zasady przetwarzania danych osobowych dzieci; niektóre z nich przedstawiono w niniejszym opracowaniu[30]. W dokumencie Komisja podkreśla z całą mocą, że dziecko zasługuje na szczególną ochronę w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, natomiast wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy na potrzeby zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania lub wykonywania kar kryminalnych oraz swobodnego przepływu takich danych nie zawiera już tak wyraźnego zapewnienia szczególnej ochrony dziecka.

Ochrona dzieci jest sprawą priorytetową, ale jest wiele problemów, które należy rozwiązać w nowym instrumencie np: kwestia udzielania zgody, dookreślenia pojęcia zgody możliwej do zweryfikowania, określenia wieku dziecka uprawniającego do udzielenia ważnej zgody, przedstawienie modelu służącego weryfikacji wieku w internecie, gdyż obecnie funkcjonujące systemy wzbudzają kontrowersje i sceptycyzm między innymi z tego powodu, że są wykorzystywane wybiórczo np. głównie podczas rejestracji na portalach hazardowych, łatwo jest sfałszować wiek, również z tego powodu, że takie systemy potrzebują dużo więcej danych (w tym wrażliwych), aby prawidłowo przeprowadzić proces weryfikacji wieku danej osoby. Kolejnymi ważnymi tematami to opracowanie modeli w zakresie form i sposobów uzyskiwania zgody od rodziców, które znajdą swoje odzwierciedlenie w kodeksów dobrych praktyk administratorów danych, a także zapewnienie skuteczniejszych środków ochrony przed aktualnymi zagrożeniami, w szczególności w Internecie. W dalszej perspektywie na poziomie prawa unijnego, a także międzynarodowego powinno się dążyć do zapewnienia dziecku łatwiejszego kontaktu z krajowym organem ochrony danych osobowych, do którego dzieci i młodzież miałyby możliwość złożenia skarg. Natomiast w sytuacjach wymagających interwencji wymiaru sprawiedliwości powinno się dążyć do zapewnienia dziecku prawa do, „przyjaznej" i bezpłatnej pomocy prawnej z poszanowaniem jego prywatności i godności.

Abstract

In her article entitled 'A Child as a subject to legal protection in the draft of the Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data', Agata Jaroszek presents the European Union reform of data protection that aims at creating modern, stable, coherent and comprehensive framework of data protection in the European Union. She describes assumptions of the Directive that provide for clarification of questionable or unclear regulations of the very Directive. Moreover, she postulates implementation of new regulations that could remarkably strengthened rights of natural persons with regard to protection of their data and control over managing and processing of personal data.

[29] W oparciu o pojęcie wprowadzone w art. 27 ust. 1 dyrektywy 95/46/WE.
[30] Stan aktualny na dzień 8 grudnia 2013 r.

ALEKSANDRA KLICH

PRAKTYCZNE ASPEKTY SPORZĄDZANIA PROTOKOŁU SKRÓCONEGO I STOSOWANIA ADNOTACJI W PROTOKOLE ELEKTRONICZNYM[1]

1. Zagadnienia wstępne

Współcześnie coraz większy wpływ na usprawnienie i przyspieszenie postępowania sądowego ma promowanie tzw. nowoczesnego modelu wymiaru sprawiedliwości, opartego przede wszystkim na wykorzystywaniu narzędzi informatycznych na rzecz usprawnienia postępowania, co niekiedy mylnie jest utożsamiane z komputeryzacją sądownictwa. Jak podkreśla się w literaturze, samo wykorzystywanie komputerów w sądach nie świadczy o informatyzacji postępowania, której głównym celem jest jego udoskonalenie poprzez wykorzystanie w praktyce zintegrowanych systemów informatycznych, a także wprowadzenie do procedury sądowej nowoczesnych narzędzi informatycznych w celu sprawniejszego dochodzenia roszczeń przed sądem[2].

Jednym z takich działań, pozytywnie wpływających na sprawność postępowania sądowego było wprowadzenie tzw. e-protokołu. W sierpniu 2010 r. Ministerstwo Sprawiedliwości w przedstawionym planie działań na 500 dni, obejmującym w szerokim zakresie kwestie związane z informatyzacją wymiaru sprawiedliwości, skierowało swą uwagę na procedury bezpośrednio związane z wdrażaniem protokołu elektronicznego, które w planie działań resortu zajmowały bardzo istotne miejsce. Założenia tego projektu, odnoszącego się także do sporządzania protokołu z posiedzenia jawnego przez utrwalanie przebiegu posiedzenia za pomocą urządzenia rejestrującego dźwięk albo obraz i dźwięk, obejmowały przede wszystkim opracowanie systemu, który byłby wykorzystywany do rejestracji przebiegu postępowania jawnego, także ogłoszenie aktów prawnych, określających sposób realizacji projektu, czego konsekwencją byłoby wdrożenie systemu w sądach apelacyjnych i okręgowych[3]. Nie bez przyczyny w tym miejscu nawiązuje się do planów działań Ministerstwa sprzed kilku lat, bowiem stanowią one doskonały punkt wyjścia do oceny obecnej praktyki sporządzania tzw. protokołu skróconego jako konstrukcji towarzyszącej stosowaniu protokołu elektronicznego.

Obecnie stoimy na progu nowelizacji przepisów odnoszących się bezpośrednio do tego protokołu pisemnego sporządzanego wraz z zapisem elektronicznym, której celem jest udoskonalenie wprowadzonych form dokumentowania pracy sądów, pozostających w zgodzie z tendencjami rozwojowymi nowoczesnego wymiaru sprawiedliwości. Wracając do momentu wdrażania protokołu elektronicznego, działania resortu skoncentrowane były na osiągnięciu podstawowych celów społecznych i ekonomicznych, do których niewątpliwie zaliczono przyspieszenie postępowań sądowych i usprawnienie funkcjonowania wymiaru sprawiedliwości, a także zwiększenie możliwości wiernego odtworzenia materiału dowodowego zgromadzonego w sprawie, zwłaszcza jeśli chodzi o przeprowadzenie dowodów, opierających się na osobowych źródłach dowodowych[4]. Ocena e-protokołu, z początku krytyczna, wiązała się z dużymi obawami wyrażanymi zarówno przez potencjalnych uczestników postępowania, ich pełnomocników, jak i przez sędziów w zakresie celowości zastosowania tego rozwiązania.

Aby dokonać rzetelnej oceny projektowanej nowelizacji art. 158 k.p.c., dotyczącej zakresu protokołu skróconego, należy przeprowadzić szczegółową i kompleksową analizę dotychczasowej praktyki sporządzania adnotacji przez sędziów sądów okręgowych i apelacyjnych. Celem niniejszego opracowania jest przedstawienie tej praktyki, a także ocena proponowanego rozszerzenia zakresu przedmiotowego protokołu skróconego. Rozważania te są o tyle istotne, że wprowadzenie i funkcjonowanie takiej konstrukcji spowodowało szereg problemów praktycznych, odnoszących się zwłaszcza do powiązania ze sobą elektronicznych i pisemnych sposobów dokumentowania przebiegu postępowania (tj. protokołu elektronicznego i protokołu skróconego).

2. Treść protokołu skróconego – założenia ustawodawcy

Zastosowanie protokołu elektronicznego dało możliwość większej koncentracji organów sądowych na przebiegu postępowania. Odgrywa on istotną rolę i zwiększa efektywność głównie w zakresie utrwalenia materiału dowodowego, bowiem wiernie odzwierciedla nie tylko czynności procesowe dokonywane przez strony, uczestników postępowania, ale i czynności świadków, czy biegłych, co odgrywa kluczową rolę z punktu widzenia koncentracji materiału procesowego. Protokół pisemny, sporządzany równolegle z protokołem elektronicznym ma formę skró-

[1] Niniejszy artykuł został przygotowany na zlecenie Prof. dr. hab. Jacka Gołaczyńskiego, Pełnomocnika Ministra Sprawiedliwości – Koordynatora Krajowego ds. wdrożeń systemów teleinformatycznych w sądach powszechnych w oparciu o projekt nowelizacji o zmianie ustawy Kodeks cywilny, ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw, przygotowany przez Ministerstwo Sprawiedliwości. W opracowaniu wykorzystano także stanowiska Pełnomocników Koordynatora Krajowego w zakresie sporządzania adnotacji w e-protokole, przesłanych Koordynatorowi Krajowemu.

[2] Por. S. Kostecka, Informatyzacja postępowania sądowego w Polsce, [w:] red. J. Gołaczyński, Informatyzacja postępowania sądowego i administracji publicznej, Warszawa 2010, s. 3-25.

[3] Skuteczny wymiar sprawiedliwości – działania Ministerstwa Sprawiedliwości na 500 dni, 2010 r., http://ms.gov.pl/Data/Files/_public/aktual/skuteczny_wymiar_sprawiedliwosci_dzialania_ministerstwa_sprawiedliwosci_na_500_dni.pdf (aktualizacja w dn. 11.12.2013 r.).

[4] Skuteczny wymiar … , op. cit. s. 18.

coną, co świadczy o jego służebnej roli względem e-protokołu. Sporządzany jest na zasadach określonych przez ustawodawcę w art. 158 § 1 k.p.c., w którym taksatywnie wskazano jego niezbędny zakres, ograniczony do informacji identyfikujących daną sprawę, m.in. zarządzeń i orzeczeń wydanych na posiedzeniu oraz stwierdzenia, czy zostały ogłoszone, a także do czynności wpływających na rozstrzygnięcie sądu (np. zawarcie ugody, zrzeczenie się roszczenia, uznanie powództwa, czy cofnięcie, zmiana, rozszerzenie lub ograniczenie pozwu) oraz do innych czynności stron, które według przepisów ustawy winny być w protokole zamieszczone.

Jak wskazano, protokół elektroniczny wiernie odzwierciedla przebieg posiedzenia, a jego skrócona forma ma charakter jedynie subsydiarny. W celu zapobieżenia konieczności przesłuchania przez sędziego całych akt sprawy, ustawodawca w rozporządzeniu z 10 sierpnia 2011 r. w sprawie zapisu dźwięku albo obrazu i dźwięku z przebiegu posiedzenia jawnego[5] upoważnił w § 9 protokolanta, działającego pod kierownictwem przewodniczącego, do sporządzania dla każdego zapisu adnotacji umożliwiających automatyczne znalezienie wskazanego jego fragmentu. Są one czynnościami o charakterze materialno-technicznym, których głównym celem jest usprawnienie dalszej pracy w odniesieniu do zapisu dokonanego w ramach protokołu elektronicznego. Mają one na celu zwiększenie czytelności i uporządkowanie elektronicznego zapisu poprzez odpowiednie ich umieszczenie w danym momencie tego zapisu, dzięki czemu nie zachodzi konieczność zapoznawania się z całym materiałem zgromadzonym na nośnikach informatycznych. Wszystkie adnotacje publiczne kwalifikowane dokonane przez protokolanta stają się integralną częścią protokołu pisemnego, zawierającego najważniejsze informacje dotyczące postępowania, a także informacje determinowane postanowieniami ustawy, tj. art. 158 § 1 k.p.c.

Protokolant może także sporządzać adnotacje, które nie zostaną ujęte w pisemnej wersji protokołu. Dotyczy to tzw. adnotacji zwykłych, których treść zawiera informacje nieujęte w art. 158 § 1 k.p.c., jak np. wypowiedzi stron i ich pełnomocników, zeznania świadków, czy przedstawiane przez biegłego tezy opinii, a także wszelkie inne informacje odnoszące się w dużej mierze do postępowania dowodowego. Adnotacje te z powodu braku urzędowego charakteru zamieszczane są na zapisie audio-wideo i co do zasady nie ma konieczności ich ujmowania w protokole pisemnym. Ich zadaniem jest stworzenie swoistego „spisu treści", którego celem jest ułatwienie odszukania odpowiedniego fragmentu nagrania zawierającego niezbędne informacje[6]. W konsekwencji tzw. adnotacje publiczne zwykłe i ich wprowadzanie do zapisu pozbawione jest obecnie obligatoryjnego charakteru, bowiem ani przepisy Kodeksu postępowania cywilnego, ani wskazanego Rozporządzenia nie określają jaki zakres informacji powinien być wprowadzony do ich treści. Zwłaszcza, że obserwowana w sądach praktyka sporządzania tzw. adnotacji publicznych zwykłych uwidacznia dużą niejednorodność w ich tworzeniu, co wpływa na konieczność wypracowania jednolitych zasad w zakresie ich tworzenia.

3. Treść protokołu skróconego w praktyce sądów

Koordynator krajowy ds. wdrożeń systemów teleinformatycznych w sądach powszechnych skierował pismo do pełnomocników powołanych w sądach apelacyjnych i okręgowych, w którym przedstawił rekomendację wypracowania jednolitych zasad odnoszących się do modelu wprowadzania adnotacji publicznych zarówno kwalifikowanych, jak i zwykłych. Działanie to podyktowane było istotnymi różnicami istniejącymi w praktyce w zakresie sporządzania protokołu skróconego, zaś celem było przeanalizowanie stosowanych rozwiązań praktycznych, przede wszystkim ustalenie czy zapisywane są jedynie krótkie adnotacje, czy wprowadzane są wprost tezy postępowania dowodowego. Odpowiedzi udzieliło jedynie 20 spośród 56 pełnomocników. W większości przypadków rekomendacja spotkała się z pozytywnym przyjęciem i akceptacją. Wyrażono także potrzebę sporządzania bardziej obszernego pisemnego zapisu przebiegu rozprawy niż ten zawierający jedynie adnotacje publiczne kwalifikowane. Sędziowie wskazywali na dużą rozbieżność w sporządzaniu adnotacji – od lakonicznych, syntetycznych adnotacji po bardzo rozbudowane, zawierające streszczenia informacji przekazywanych przez uczestników postępowania, jak i świadków (np. Sąd Okręgowy w Lublinie, Poznaniu, Tarnowie). Zdarzały się jednak głosy negujące treść proponowanej rekomendacji, wskazujące na brak możliwości wypracowania jednorodnego modelu ze względu na zbyt duże rozbieżności pomiędzy sędziami (np. Sąd Okręgowy w Koszalinie), a także ze względu na wypracowanie przez sędziów własnego modelu tworzenia adnotacji, opartego na zakresie wskazanym w art. 158 § 1 k.p.c. (np. Sąd Okręgowy w Opolu) .

Wyniki przeprowadzonej analizy pozwalają na wyodrębnienie trzech zasadniczych podejść, prezentowanych obecnie w sądach w odniesieniu do kształtowania treści protokołu skróconego, a w szczególności do sporządzania adnotacji. Wyróżnić należy podejście skrajnie syntetyczne, podejście syntetyczne z elementami opisu oraz podejście opisowe.

Pierwsze z nich, tj. podejście skrajnie syntetyczne, wręcz minimalistyczne przejawia się w tym, że adnotacje stanowią jedynie punkty dzielące protokół na wyodrębnione zgodnie z intencją sędziego fragmenty. Protokół skrócony w takich przypadkach ogranicza się do niezbędnego minimum, a jego zasadniczą funkcją jest jedynie uporządkowanie poszczególnych części protokołu zasadniczego (elektronicznego). Oznacza to, że protokół w takich sytuacjach odzwierciedla zaledwie niezbędne detale ściśle wynikające z przepisów prawa, tj. art. 158 § 1 k.p.c., a więc zawiera informacje zawężone do wskazania tożsamości uczestników rozprawy zabierających głos. Przygotowywanie protokołu skróconego zgodnie z podejściem syntetycznym wskazuje więc na wykorzystywanie go przez sędziów w celu wykonywania funkcji porządkującej. Podejście to w praktyce sądów samodzielnie występuje sporadycznie (np. Sąd Okręgowy w Opolu). Zdecydowanie częściej mamy do czynienia z mniej lub bardziej zaakcentowanymi elementami osobowymi w protokole skróconym.

Dlatego też należy uznać, że podejście syntetyczne z elementami opisu, jest dominujące w obecnej praktyce (np. Sąd Okręgowy w Białymstoku, Łodzi, Rzeszowie, Siedlcach, Świdnicy). Nie ogranicza się ono do funkcji porządkującej protokołu skróconego. Takiemu podejściu daje wyraz wprowadzanie przez sędziów elementów opisowych, a tym samym w pewnym zakresie

[5] Dz.U. z 2011 r., nr 175, poz. 1046.

[6] Por. J. Gołaczyński, Przewodnik po e-protokole, „Na wokandzie", 2011, nr 6, s. 30-31.

w protokole skróconym włączane są te elementy treści, które dotychczas znane były tradycyjnej formie protokołu pisemnego. Adnotacje w tych przypadkach rozbudowywane są o tezy zeznań świadków, czy wyników postępowania dowodowego, co zasługuje na aprobatę w sytuacji, gdy działania te są w pełni uświadomionymi decyzjami sędziów, uwzględniającymi to, że adnotacje nie stanowią tradycyjnego protokołu, a jedynie – materiał pomocniczy, pełniący funkcję subsydiarną wobec pełnej wersji e-protokołu (np. Sąd Okręgowy w Łodzi). Wskazana funkcja opisowa protokołu skróconego wykorzystywana jest w omawianych przypadkach przez sędziów w różnorodny sposób. W praktyce stosowane są przez sędziów zapisy dotyczące wyników lub samych tez postępowania dowodowego, w szczególności w sytuacji, gdy opierają się na osobowych źródłach dowodowych (np. Sąd Okręgowy w Rzeszowie), a niekiedy przybierają wręcz formę obszernych adnotacji publicznych (np. Sąd Okręgowy w Siedlcach). Istotny jest przy tym fakt, iż obszerność treści adnotacji odnoszących się do wyników postępowania dowodowego, czy wyjaśnień informacyjnych stron nie pełni w tym wypadku roli streszczenia. Działanie to bowiem nadal ogranicza się do realizacji funkcji porządkującej w nieco szerszym zakresie, co należy ocenić pozytywnie. Ma ono na celu zwiększenie przejrzystości protokołu elektronicznego, co osiągane jest poprzez zastosowanie tzw. węzłowych treści i uproszczonej konstrukcji zapisywanych informacji. W niektórych sytuacjach od decyzji przewodniczącego uzależnione jest to, czy adnotacje te przenoszone są do protokołu skróconego (np. Sąd Apelacyjny i Sąd Okręgowy w Białymstoku). Różnorodność sposobu wykorzystywania w praktyce rozwiązania syntetycznego z elementami opisu niewątpliwie uzależniona jest w głównej mierze od poziomu skomplikowania danej sprawy, ponieważ wskazane elementy opisowe w protokole wykorzystywane są przez niektórych sędziów jedynie w sprawach o skomplikowanym charakterze, natomiast inni robią to w zasadzie w każdej sprawie.

Należy podkreślić, że najczęściej w praktyce sądów dostrzegalne jest to łączenie obu funkcji protokołu skróconego (funkcji porządkującej i opisowej) przede wszystkim ze względu na charakter danej sprawy (np. Sąd Okręgowy w Gliwicach, Nowym Sączu, Przemyślu, Szczecinie). Zasadą jest, że w tzw. sprawach prostych zachodzi tworzenie adnotacji w rozumieniu art. 158 § 1 k.p.c., ograniczających się do oznaczenia tożsamości uczestników postępowania i osób biorących w nim udział, czy osnowy zgłoszonych wniosków. Natomiast w sprawach o skomplikowanym charakterze, istotną rolę odgrywa wskazana funkcja opisowa, choć ograniczona do niezbędnych rozmiarów, zwłaszcza w zakresie skoncentrowanego w sprawie i przedstawionego materiału dowodowego.

Takie podejście wiąże się jednak z określonymi problemami praktycznymi. Dlatego też należy zwrócić uwagę na to, iż umieszczanie w adnotacjach zwykłych kilkuzdaniowych streszczeń z postępowania dowodowego może stanowić podstawę do zgłaszania wniosków o sprostowanie protokołu z uwagi na to, że mogą one wypaczać wypowiedzi, a nawet pozostawać w sprzeczności z zapisami protokołu elektronicznego (na co wskazuje także pełnomocnik w Sądzie Okręgowym w Gliwicach). W tym przypadku protokół skrócony mógłby być nie tylko pozbawiony swego subsydiarnego charakteru, ale stanowić utrudnienie dla odtworzenia rzeczywistego przebiegu postępowania (mimo swego istnienia powodować konieczność przesłuchania całości materiału elektronicznego). Pozytywnie zaś należy ocenić zapisywanie ogólnych informacji, odnoszących się do tez związanych z materiałem dowodowym, co niewątpliwie pozytywnie wpłynie na późniejszą pracę sędziego zmierzającą do wypracowania trafnego orzeczenia.

Trzecie z podejść zauważonych w praktyce to takie, w którym eksponuje się funkcje opisowe protokołu skróconego. W konsekwencji *de facto* protokół skrócony staje się odzwierciedleniem protokołu tradycyjnego, sporządzanego w sytuacji, gdy wyłączona jest możliwość sporządzenia protokołu elektronicznego (art. 158 § 2 k.p.c.), bowiem stanowi on pełny zapis tego, co dzieje się na sali sądowej. Tak szerokie zastosowanie elementów opisowych podważa sens wprowadzenia e-protokołu, bowiem jego charakter sprowadza się do roli weryfikującej prawdziwość protokołu skróconego, a to stanowi rozwiązanie niedopuszczalne zarówno na gruncie prawa cywilnego procesowego, jak i ze względów prakseologicznych. W tym modelu wyraźnie funkcja opisowa wyprzedza funkcję porządkującą, a ta ostatnia powinna prawidłowo określać sens istnienia protokołu skróconego. Podejście opisowe w czyste formie występuje w nielicznych przypadkach i uwidocznione jest przede wszystkim w sprawach o bardzo skomplikowanym stanie faktycznym. W takich sytuacjach adnotacje stanowią pełny zapis zeznań stron, czy świadków, zaś sędziowie starają się, aby tezy w nich zawarte odzwierciedlały sformułowania uczestników procesu. Co więcej, wskazywana w odpowiedziach w pełnomocników, obawa sędziów przed potraktowaniem streszczeń, czy też wypowiedzi uczestników postępowania jako wstępnej oceny materiału dowodowego generuje potrzebę pełnego odzwierciedlania wypowiadanych przez nich twierdzeń w adnotacjach (np. Sąd Okręgowy w Częstochowie, Piotrkowie Trybunalskim).

Takie podejście powoduje powrót do tradycyjnego modelu protokołu, co prowadzi do zachwiania subsydiarnego charakteru protokołu skróconego względem e-protokołu. Należy pamiętać o tym, iż adnotacje mają charakter pomocniczy, wykorzystywany dla celów protokołu elektronicznego, a ich zadaniem z pewnością nie jest wierne odzwierciedlenie twierdzeń zapisanych na nośnikach informatycznych, a jedynie ułatwienie szybszego dotarcia do ich poszczególnych fragmentów. Zapisywanie w formie adnotacji pełnych treści zeznań stron, świadków, czy biegłych, potwierdzonych nagraniem w protokole elektronicznym prowadzić może do bieżącej transkrypcji. W przypadku takiego działania zapomnieniu ulega rzeczywista rola protokołu skróconego, który przypominając w swej treści protokół tradycyjny przestaje być porządkującym e-protokół. Takie podejście stanowi zaprzeczenie idei przyspieszenia i usprawnienia postępowania sądowego.

Należy podkreślić, że analizę omawianego zagadnienia utrudnia również fakt, że skrajne przypadki w praktyce sądów wskazują na łączenie podejścia syntetycznego z opisowym nawet w obrębie tych samych jednostek organizacyjnych (np. Sąd Okręgowy w Tarnowie). Zauważalna jest duża rozbieżność – od lakonicznych syntetycznych adnotacji, po bardzo rozbudowane, zawierające wierne odzwierciedlenie informacji przekazywanych przez uczestników postępowania. Zarówno taka postawa, jak i stanowiska sędziów wskazujące na brak możliwości wypracowania jednorodnego modelu w zakresie sporządzania adnotacji publicznych zwykłych i treści protokołu skróconego jednoznacznie wskazują na konieczność wprowadzenia ujednoliconej formy sporządzania adnotacji publicznych zwykłych. Oczywiście nie

jest możliwe kategoryczne wprowadzenie takiego rozwiązania, pozbawiające sędziego możliwości dokonania indywidualnej analizy stanu faktycznego i związanego z tym odpowiedniego dokonania adnotacji. Zasadnym jest natomiast dążenie do wypracowania podstawowych standardów w tej materii.

4. Uwagi *de lege ferenda*

Projektowana nowelizacja art. 158 § 1 k.p.c.[7] służy rozszerzeniu treści protokołu skróconego, poprzez dodanie §1[1], w świetle którego dopuszczalne będzie zawieranie wniosków i twierdzeń stron, wyników postępowania dowodowego oraz innych okoliczności istotnych dla przebiegu posiedzenia. Proponowane przez Ministerstwo Sprawiedliwości rozwiązanie co do rozszerzenia zakresu adnotacji zwykłych wydaje się być racjonalnym, o ile nie zostanie odczytane przez sędziów w praktyce jako przyzwolenie do reprezentowania omówionego trzeciego podejścia, skrajnie opisowego, sprowadzającego charakter treści protokołu skróconego do zakresu pełnego protokołu elektronicznego. Projektowana nowelizacja w rzeczywistości stanowiłaby w dużym stopniu odzwierciedlenie w przepisach prawa już upowszechnionej praktyki o stosowaniu tzw. adnotacji zwykłych, odnoszących się do postępowania dowodowego, zwłaszcza w sprawach o skomplikowanym charakterze, przez co możliwe będzie nadanie tym adnotacjom statusu adnotacji publicznych kwalifikowanych. Rządowy projekt nowelizacji także w odniesieniu do zachowania samodzielności sędziów w zakresie sporządzania adnotacji należy ocenić pozytywnie. Projektowana konstrukcja nie zobowiązuje bowiem sędziego do dokonania takiej adnotacji, ale daje podstawę prawną do jej sporządzenia, co niewątpliwie pozostaje w zgodzie z przyjętym w Kodeksie postępowania cywilnego modelem dyskrecjonalnej władzy sędziego.

Należy jednak zauważyć, że w uzasadnieniu do projektowanej nowelizacji wskazano, iż protokół skrócony będzie mógł obejmować taką samą treść, jak tradycyjny protokół pisemny, co ułatwi i przyspieszy zapoznanie się z przebiegiem posiedzenia. W mojej opinii takie ujęcie problemu zasługuje na krytykę, ponieważ zrównanie stopnia szczegółowości protokołu skróconego z treścią protokołu elektronicznego stanowiłoby krok wstecz, niwelujący prakseologiczne uzasadnienie wprowadzenia protokołu elektronicznego. O ile tożsamość w zakresie elementów treści protokołów jest pożądana, o tyle metoda odzwierciedlenia treści powinna być odmienna, ponieważ winna koncentrować się na istocie tych elementów, przy pełnej realizacji wskazanej wyżej funkcji porządkującej protokołu skróconego.

Reasumując rozważania w tym zakresie, podkreślić należy, iż istotnym zagrożeniem jest stopień szczegółowości informacji zawartych w adnotacjach, zwłaszcza w sprawach o skomplikowanym stanie faktycznym. O ile zastosowanie modelu pierwszego (syntetycznego) nie budzi zagrożeń, bo jest w pełni zgodne z regulacją zawartą w art. 158 § 1 k.p.c., to granica pomiędzy modelem syntetycznym z elementami opisu, a modelem opisowym jest bardzo płynna, a jej przekroczenie nieść może za sobą poważne konsekwencje, poddające w wątpliwość istotę wprowadzenia protokołu elektronicznego. Stać się tak może, gdy w sytuacji dużego skomplikowania stanu faktycznego sędzia nie ograniczy się do zawarcia w adnotacjach najważniejszych informacji dotyczących wyników postępowania dowodowego, zalecając protokolantowi zapisywanie dokładnej lub sparafrazowanej treści informacji pochodzących od osobowych źródeł dowodowych. Przedmiotem wątpliwości nie powinny być w tej sytuacji podnoszone argumenty o możliwym dokonaniu przez sędziego wstępnej oceny materiału dowodowego, co zostanie ujawnione w adnotacji publicznej, ale ryzyko pozbawienia protokołu skróconego charakteru porządkującego względem e-protokołu, bowiem z pewnością protokół skrócony nie może być kolejnym pełnym odzwierciedleniem przebiegu postępowania.

Uproszczona forma protokołu sporządzana wraz z adnotacjami w rozumieniu wskazanego podejścia syntetycznego służyć ma lepszej orientacji w zapisie audio-wideo. Argumentacja ta zasługuje w pełni na uwzględnienie, a przede wszystkim na upowszechnienie, zwłaszcza wśród sędziów umniejszających rolę e-protokołu. Sędziowie ci ograniczają jego znaczenie do roli weryfikatora zapisu znajdującego się w protokole skróconym, tym samym utożsamiając ten drugi z tradycyjną formą protokołu pisemnego. Konsekwencją tego nie jest rzeczywiste skrócenie czasu postępowania (poprzez odejście od dyktowania treści zeznań do protokołu), ale pozostawienie swoistej transkrypcji „na żywo", która w razie ewentualnych rozbieżności może być weryfikowana i poprawiona poprzez przesłuchanie materiału elektronicznego.

Na gruncie obowiązującego prawa, zwłaszcza art. 158 § 1 k.p.c. uwidoczniony jest brak przepisów „wymuszających" zapisywanie w protokole skróconym treści wykraczających poza zakres adnotacji publicznych kwalifikowanych, wobec czego zachodzi potrzeba sporządzenia bardziej obszernego pisemnego zapisu przebiegu rozprawy. Adnotacje te powinny mieć jednak charakter swoistego „spisu treści", co jednoznacznie wskazywałoby na realizację funkcji porządkującej. Istotne jest to, aby wprowadzana była uproszczona konstrukcja informacji o tym czego dotyczy dany fragment zapisu, a nie – co zostało wypowiedziane. Współcześnie dostrzegalna jest potrzeba wypracowania modelu pośredniego, opartego na podejściu syntetycznym z elementami opisu, wyłączającego obszerność zapisów dotyczących dosłownego oddania wypowiedzi uczestników postępowania.

W mojej opinii najbardziej pożądane byłoby, gdyby przy sporządzaniu protokołu skróconego zachowana była dominująca funkcja porządkująca z niezbędnymi elementami opisu. Na uwagę zasługuje ponadto fakt, iż te opisowe elementy powinny odnosić się do spraw o bardziej skomplikowanym stanie faktycznym. Decydowanie o częstotliwości i zakresie treści adnotacji pozostaje w rękach przewodniczącego, działającego w ramach dyskrecjonalnej władzy sędziego. Tym samym w ramach poszanowania zasady swobodnej oceny dowodowej powinien być zachowany także aspekt swobodnego, skróconego dokumentowania tego postępowania odzwierciedlonego w pełnej formie protokołu elektronicznego. Swoboda nie oznacza jednak dowolności pracy sędziego, zmierzającej do swoistego „dublowania" udokumentowania przebiegu rozprawy. Nie należy zapominać o tym, iż protokół skrócony stanowi podstawowe narzędzie pracy sędziego, spełniając przy tym pomocniczą rolę względem e-protokołu, bo pozwala na konfrontację treści adnotacji z pełnym zapisem odzwierciedlonym na nośnikach informatycznych.

[7] Projekt Ustawy o zmianie ustawy – Kodeks cywilny, ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw, http://legislacja.rcl.gov.pl/docs//2/177283/177292/177293/dokument84467.pdf?lastUpdateDay=06.12.13&lastUpdateHour=16%3A04&userLogged=false&date=niedziela%2C+8+grudzie%C5%84+2013 (aktualizacja w dn. 12.12.2013 r.)

Należy pamiętać także o tym, że samo zapisanie wyników postępowania dowodowego w formie adnotacji, co pozostaje w zgodzie z projektowaną nowelizacją art. 158 k.p.c., nie jest równoznaczne z odzwierciedleniem szczegółowych tez, czy streszczaniem wypowiedzi stron, świadków, biegłych etc. Dobrą i pożądaną praktyką byłoby odzwierciedlanie w adnotacjach funkcji porządkującej, jaką winny spełniać. Ponadto w ramach pozytywnej oceny proponowanej nowelizacji art. 158 k.p.c., zwrócić należy uwagę na będące jej celem uproszczenie pracy sędziów, a także ułatwienie kontynuowania tej pracy w przypadku przejmowania sprawy.

Abstract

Aleksandra Klich describes 'Practical aspects of drawing up an abbreviated minutes of a court session and using annotations in the electronic protocol'. The article aims at presenting a detailed and comprehensive analysis of the practical aspects of making the annotations in question by judges of regional courts and courts of appeal, and at evaluating suggested expansion of the thematic scope of the abbreviated minutes of a court session. It is possible to conclude that introducing and functioning of such legal construction resulted in a wide range of practical problems that particularly refer to matching electronic and traditional methods of documenting the course of court sessions (i.e. electronic and abbreviated minutes).

MARCIN SZURPICKI

PROBLEMATYKA ANONIMOWOŚCI W SIECI, CZYLI JAK DOTRZEĆ DO PODMIOTU NARUSZAJĄCEGO PRAWO W INTERNECIE

1. Wstęp

W XXI wieku Internet stał się najpopularniejszą formą komunikacji. Rozwój technologii sprawił, że człowiek jest wręcz uzależniony od korzystania z Internetu. Potrzeba dostępu do Sieci została przez kraje wysoko rozwinięte uznana za jedno z podstawowych praw człowieka[1], a ciągłe poszerzanie zasięgu sieci teleinformatycznych sprawia, że ciężko znaleźć miejsce, w którym nie można by sprawdzić poczty elektronicznej czy najnowszych wiadomości[2].

Ograniczenie pojęcia „Internetu" do samej tylko komunikacji byłoby niesprawiedliwym zawężeniem. Wydaje się, że słuszniejszym jest uznanie go za alternatywne pole działania, niejako zastępcze dla działania w świecie rzeczywistym. Coraz szerszy wachlarz oferowanych usług wraz z łatwością korzystania i oszczędnością czasu, sprawiają, że to przy użyciu Internetu załatwiane jest coraz więcej spraw życia codziennego. Co więcej pojawia się tendencja do wypierania tradycyjnych zachowań na rzecz czynności dokonywanych za pomocą Sieci[3].

Internet bezsprzecznie uznać można za jedno z największych osiągnięć technicznych, a nawet symbol naszych czasów. Jednak każde wielkie osiągnięcie pociąga za sobą możliwości wykorzystania go w znacznie odmienny sposób niż pierwotnie zakładano. Obok wszystkich plusów, funkcjonowanie w Internecie pociąga za sobą ogromną liczbę zagrożeń. Pomimo, iż działanie (a w szczególności konsekwencje działania) w Sieci nie różnią się niczym od działania w świecie rzeczywistym, niemal na każdym kroku spotkać można przykłady łamania prawa. Sytuacja taka wiąże się z poczuciem bezpieczeństwa sprawców i ich pozorną anonimowością.

Przed pojawieniem się Internetu sprawca naruszenia prawa był względnie łatwy do zidentyfikowania. Jak jednak dotrzeć do osoby, przykładowo umieszczającej znieważający wpis na stronie Internetowej, gdy jedyną informacją jaką o niej posiadamy jest jej wymyślony, fikcyjny pseudonim? Co więcej, nawet gdyby pokrzywdzony chciał otrzymać chociaż minimalny zakres informacji o danym podmiocie, prawo często stoi na straży osób naruszających prawo (dość paradoksalnie), chroniąc ich prywatność i zapewniając względną anonimowość.

To właśnie poczucie bezpieczeństwa jest głównym czynnikiem, wpływającym na wzrost przypadków łamania prawa w Sieci. Możliwość uniknięcia kary sprawia, że ludzie chętniej niż dotychczas naruszają przepisy tak prawa karnego jak i cywilnego. W rzeczywistości anonimowość[4] w Internecie jest jednak fikcją niedającą żadnej gwarancji bezpieczeństwa.

Celem niniejszego artykułu jest wskazanie różnych możliwości dotarcia do podmiotu naruszającego prawo przy użyciu Internetu. Przepisy gwarantujące ochronę danych osobowych i prywatności przy zastosowaniu odpowiednich instytucji można obejść i finalnie dotrzeć do konkretnego użytkownika Sieci. Materiał opracowania został podzielony na dwie części: pierwszą, w której opisane zostały instytucje prawa karnego i drugą poruszającą kwestie prawa cywilnego. Rozdzielenie takie jest konieczne, albowiem o ile część spraw już z mocy prawa zostanie poddana przepisom prawnocywilnym lub prawnokarnym, w niektórych sytuacjach (szczególnie w przypadku naruszenia godności czy czci), to do pokrzywdzonego będzie należał wybór ścieżki, którą się posłuży. Związany on będzie z możliwymi roszczeniami przysługującymi pokrzywdzonemu, różnymi sposobami dotarcia do anonimowego sprawcy oraz czynnikami wpływającymi na rozwój sprawy.

2. Określenie podmiotu naruszającego prawo w Internecie przy zastosowaniu przepisów prawa karnego

Przestępstwa popełniane w sieci, ścigane na gruncie prawa karnego, podzielić należy na dwie grupy. Po pierwsze będą to przestępstwa ścigane w trybie publicznoskargowym, a więc ścigane z urzędu lub na wniosek pokrzywdzonego. Mając na uwadze zagrożenia z jakimi wiąże się funkcjonowanie człowieka w Internecie, prawodawca wprowadził do ustawy szereg przepisów związanych z Siecią. Najprostszym przykładem są chociażby art. 190a i 191a Kodeksu Karnego (ścigane na wniosek) oraz 200a czy 287 k.k. (ścigane z urzędu). Objęcie tych przestępstw trybem publicznoskargowym jest znacznym ułatwieniem dla pokrzywdzonych w dochodzeniu swoich praw. Wystarczy bowiem aby penalizowany czyn wystąpił lub został złożony wniosek pokrzywdzonego o jego ściganie, aby cała procedura prawna ruszyła, nawet bez dalszych, aktywnych działań ze strony pokrzywdzonego. To organy władzy państwo-

[1] Np. w Finlandii, prawo do szerokopasmowego Internetu (z prędkością powyżej 1 Mb/s) zostało uznane za podstawowe prawo człowieka por. Ł. Matuszewski, Finlandia – Internet szerokopasmowy prawem każdego Fina, http://www.twojaeuropa.pl/962/finlandia-internet-szerokopasmowy-prawem-kazdego-fina, [dostęp 06.12.2013]

[2] Przykładowo w Estonii, niemal na całym terytorium kraju, można bezpłatnie połączyć się z Internetem, za pomocą urządzenia odbierającego sygnał Wi-Fi, por. http://www.rp.pl/artykul/937760.html [dostęp 03.12.2013]

[3] Obsługa studiów przy pomocy programów internetowych (np. UsosWeb), wymóg internetowej rejestracji kandydatów na studia (np. IRKA), wypieranie tradycyjnej poczty przez usługi poczty elektronicznej

[4] Dla celów artykułu, pojecie „anonimowości" użyte zostanie w znaczeniu braku możliwości odpowiedniego określenia podmiotu naruszającego przepisy prawa (jego imienia, nazwiska, fizycznego adresu).

wej zobowiązane są do dochodzenia sprawiedliwości i na nie zostaje przerzucony ten trud. Warto w tym miejscu wspomnieć o fakcie, iż ogromna ilość przepisów prawa karnego, nawet bezpośrednio nie powiązana z funkcjonowaniem w Internecie, może być zastosowana do działań w Sieci (np. 190 k.k.)

Drugą grupę stanowią przestępstwa ścigane w trybie prywatnoskargowym i to ta grupa będzie głównym tematem dalszych rozważań, albowiem w trybie tym na pokrzywdzonego przeniesione zostają główne ciężary związane z postępowaniem. Grupa przestępstw ściganych w tym trybie jest wprost określona w Kodeksie Karnym. Także tutaj dokonać należy swoistej dyferencjacji na przestępstwa związane z naruszeniem integralności ciała (157 par. 2 k.k., 157 par. 3 k.k., 157 par. 4 k.k,, 217 par. 3 k.k.), zniesławienie (art. 212 par. 1 i 2 k.k.) oraz zniewagę (art. 216 par. 1 i 2 k.k.). Z oczywistych względów problematyka naruszenia czy uszkodzenia ciała zostanie w dalszych rozważaniach pominięta, ponieważ nie sposób doszukać się możliwości (bezpośredniego) popełnienia któregoś z tych przestępstw przy użyciu Internetu. Reasumując, problem związany dotarciem do „anonimowego" sprawcy przestępstw na gruncie prawa karnego, będzie związany tylko ze spełnieniem przesłanek określonych w art. 212 i 216 k.k..

Wszczęcie postępowania z oskarżenia prywatnego polega na wniesieniu przez pokrzywdzonego prywatnego aktu oskarżenia. Ustawa wskazuje na minimalne wymagania stawiane takiemu aktowi, ograniczając je do oznaczenia osoby oskarżonego, wskazania zarzucanego mu czynu oraz podania dowodów, na których opiera się oskarżenie[5]. Zastosowanie art. 487 k.p.k. w sprawach, w których miejscem działania jest Internet napotyka jednak niezwykłe trudności. Abstrahując od aspektów czynu zabronionego popełnianego w Sieci oraz problematyki związanej z zebraniem i zabezpieczeniem dowodów cyfrowych (które wymagają osobnego opracowania), największą przeszkodą jest właśnie wskazanie sprawcy przestępstwa.

Ustawa, jako jeden z wymogów formalnych prywatnego aktu oskarżenia, wskazuje *oznaczenie osoby oskarżonego*. Odpowiednie oznaczenie powinno posiadać imię, nazwisko i adres zamieszkania oskarżonego[6]. Jednak doktryna coraz częściej schyla się ku stanowisku, że wystarczające jest podanie adresu miejsca pracy oskarżonego lub innego, na który możliwe będzie przesłanie mu korespondencji[7]. Jak łatwo zauważyć, tak sformułowany przepis doznaje znacznego ograniczenia w środowisku elektronicznym. Pokrzywdzony może posiadać dane lub mieć możliwość zdobycia dokładnych danych tylko pewnej, ograniczonej liczby znanych mu podmiotów. Co więcej tylko niewielki odsetek portali internetowych wymaga od użytkowników podania imienia i nazwiska (głównie portale społecznościowe, portale informacyjne, elektroniczne wydania gazet – wszędzie gdzie podanie autora zamieszczonego tekstu jest niezbędne). Niemniej jednak sugerowanie się ich prawdziwością, przy częstym braku jakiejkolwiek weryfikacji pod kątem ich prawdziwości, byłoby sporym ryzykiem. Nie należy także zapominać, że użytkownicy Sieci zazwyczaj posługują się fantazyjnymi *nickami*, pseudonimami czy loginami, które w żaden sposób nie wskazują konkretnej osoby. Nie podlega dyskusji fakt, iż pseudonim nie może być traktowany jako odpowiednie oznaczenie oskarżonego, a co za tym idzie jego podanie jest niewystarczające do wniesienia prywatnego aktu oskarżenia.

Postępowanie w trybie prywatnoskargowym może być również wszczęte na podstawie pisemnej lub ustnej skargi, złożonej przez pokrzywdzonego Policji[8]. Artykuł 488 par. 1 k.p.k. wprost wskazuje, że Policja ma obowiązek skargę taką przyjąć, a w razie potrzeby zabezpieczyć dowody i przekazać ją do właściwego sądu[9]. Podobnie jak w poprzednim przypadku, także przy skardze pojawiają się problemy związane z oznaczeniem oskarżonego. Zważywszy na brak określenia przez prawodawcę różnic między skargą a prywatnym aktem oskarżenia (a w szczególności braku sprecyzowania wymogów odpowiedniego oznaczenia oskarżonego), kwestia ta jest od dawna elementem sporu w doktrynie. Część autorów opowiada się za stanowiskiem, iż wymogi formalne skargi są takie same jak wymogi prywatnego aktu oskarżenia z art. 487 k.p.k.[10], a więc odpowiednie oznaczenie oskarżonego polegać będzie na wskazaniu jego imienia, nazwiska i adresu korespondencyjnego. Autorzy stojący w opozycji do tej tezy podkreślają, że nie bez przyczyny prawodawca wprowadził rozróżnienie na „prywatny akt oskarżenia" oraz „skargę", a także podkreślają, że skarga jest pojęciem znacznie szerszym od aktu oskarżenia i nie można wymagać od niej wszystkich jego wymogów formalnych[11]. Stanowisko takie jest zresztą zgodne z orzecznictwem Sądu Najwyższego, który wyraźnie stwierdził, że *„(skarga) jest pojęciem szerszym i mniej sformalizowanym, mającym podobne znaczenie procesowe jak zawiadomienie o przestępstwie, które – co oczywiste – może odnosić się także do anonimowego sprawcy, którego ustalenie może nastąpić przez Policję"*[12]. Idąc tym tokiem rozumowania wydaje się, że druga teza jest słuszniejsza, zwłaszcza uwzględniając specyfikę środowiska internetowego. Przyjęcie odmiennego stanowiska pozbawiłoby pokrzywdzonego realnej możliwości dochodzenia swoich praw[13]. Reasumując, samo złożenie skargi na Policji jest wystarczające dla wszczęcia postępowania w trybie prywatnoskargowym, nawet gdyby pokrzywdzony nie był w stanie dokładnie określić danych personalnych osoby naruszającej jego prawa.

Ustalenie przez Policję danych sprawcy czynu zabronionego polega na uzyskaniu adresu IP komputera, z którego dokonano danego czynu, a dzięki tym informacjom dotarcie do konkretnego użytkownika. Numer IP jest jednak objęty tajemnicą komunikacyjną określoną w Ustawie Prawo Telekomunikacyjne[14], a uchylenie jej następuje dopiero na podstawie postanowienia sądu lub prokuratora (art. 159 par. 4 u.pr.tel.). Postanowienie takie wydawane jest na podstawie art. 488 par. 2 k.p.k., bądź po wniesieniu prywatnego aktu oskarżenia do właściwego sądu (w tym wypadku w celu zabezpieczenia dowodów), lub na dodatkowy wniosek Policji składany wraz ze skargą z art. 488 par.1 k.p.k. (w celu ustalenia personaliów osoby łamiącej prawo). W odniesieniu do popełnienia czynu zabronionego w Internecie, niezwykle istotne wydają się także uprawnienia pły-

[5] Art. 487 k.p.k.

[6] T. Grzegorczyk, Kodeks postępowania karnego. Komentarz, Kraków 2003, s 1245

[7] Z. Banasiak, Przyjęcie zawiadomienia o przestępstwie prywatnoskargowym w praktyce policyjnej, [w:] Prokuratura i Prawo 7-8 2010, Kraków 2010, s. 226

[8] T. Grzegorczyk, J. Tylman, Polskie postępowanie karne, Warszawa 2009, s. 838

[9] Z. Banasiak, Przyjęcie zawiadomienia o.... s. 229

[10] Por. T. Grzegorczyk, J. Tylman, Polskie postępowanie…, s. 838

[11] Z. Banasiak, Przyjęcie zawiadomienia o...., s. 229

[12] Postanowienie Sądu Najwyższego z dnia 17 kwietnia 1997 r., sygn. I KZP 4/97

[13] Nieodpowiednie oznaczenie oskarżonego traktowane jest jako brak formalny, i powoduje zwrot aktu oskarżenia oskarżycielowi (art. 332, art. 337 k.p.k.)

[14] Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne, (Dz.U. 2004 nr 171 poz. 1800)

nące z art. 308 k.p.k.[15]. Zgodnie z nim, w granicach koniecznych do zabezpieczenia śladów i dowodów przestępstwa przed ich utratą, zniekształceniem lub zniszczeniem, prokurator albo Policja może w każdej sprawie, w wypadkach niecierpiących zwłoki, przeprowadzić w niezbędnym zakresie czynności procesowe[16]. Wydanie postanowienia o uchyleniu tajemnicy komunikacyjnej może znacznie przedłużać postępowanie, a zważywszy na łatwość usunięcia lub zmodyfikowania treści w Internecie, naraża na utratę istotnych dowodów. Uprawnienia przewidziane w art. 308 k.p.k. pozwalają Policji zabezpieczyć dane, jeszcze przed wydaniem odpowiedniego postanowienia, co w należyty sposób zabezpiecza postępowanie.

Wydanie odpowiedniego postępowania zezwala Policji na dokonanie wszelkich czynności rozpoznawczych zmierzających do określenia sprawcy czynu zabronionego. Już samo uzyskanie numeru IP pozwala na dotarcie do konkretnego komputera, ustalenie jego fizycznego adresu, a w praktyce odnalezienie i określenie sprawcy czynu zabronionego,

3. Określenie podmiotu naruszającego prawo w Internecie przy zastosowaniu przepisów prawa cywilnego

W odróżnieniu od prawa karnego, na gruncie prawa cywilnego pokrzywdzony jest głównym aktorem postępowania. Do niego należy zainicjowanie postępowania (poprzez wniesienie pozwu) oraz ciężar przytoczenia wszystkich dowodów, koniecznych do poparcia swojego roszczenia (art. 6 Kodeksu Cywilnego). Wobec tego nie ma konieczności wprowadzania tu dodatkowego rozróżnienia sytuacji naruszenia prawa, która zastosowana była przy zarysowaniu problematyki na gruncie prawa karnego.

Jednym z kluczowych elementów każdego pozwu jest odpowiednie oznaczenie stron sprawy. Kodeks Postępowania Cywilnego precyzuje, że oznaczeniami są imię i nazwisko lub nazwa (w przypadku osoby prawnej) (art. 187 par. 1, art. 126 par 1 pkt 1 k.p.c.). Oczywistym jest, że adresatem roszczeń nie może być osoba fizyczna oznaczona tylko przy pomocy jej pseudonimu. Co więcej sugerowanie się, że pod danym *nickiem* ukrywa się konkretny podmiot, mogłoby doprowadzić do pozwania osoby całkowicie niezwiązanej ze sprawą[17]. W tej sytuacji, tak jak w przypadku postępowania karnego, jedyną możliwością dotarcia do anonimowego użytkownika, jest próba odnalezienia go po *traffic data*[18].

Przyjmuje się, że na gruncie ustawy o ochronie danych osobowych (art. 6) i dyrektywy 2002/58/WE (art. 2) adres IP uważany jest za dane osobowe[19]. Co więcej zaryzykować można stwierdzenie, że pozostałe *traffic data,* także powinny podlegać ochronie zbliżonej do ochrony adresu IP**.** W związku z tym ich przetwarzanie, przechowywanie i udostępnianie podlega restrykcyjnym regułom określonym w ustawie o ochronie danych osobowych. Administratorem danych osobowych, w przypadku naruszenia dóbr osobistych w Internecie, w większości przypadków będzie *service provider*[20] (np. administrator danego portalu) i do niego powinny być kierowane roszczenia o ujawnienie danych osobowych użytkownika naruszającego prawo.

Do niedawna drogą dochodzenia swoich praw przez pokrzywdzonych był art. 29 Ustawy o Ochronie Danych Osobowych[21]. Na jego podstawie administrator danych był zobowiązany do udostępnienia danych osobowych podmiotowi, któremu uprawnienie takie przysługiwało na mocy przepisów prawa. Dane osobowe mogły być również udostępniane innym osobom, jeżeli w sposób wiarygodny uzasadniły potrzebę ich posiadania (np. pokrzywdzonemu pragnącemu wnieść pozew odpowiedniej treści, w celu odpowiedniego określenia pozwanego), a ich udostępnienie nie spowodowało naruszenia praw i obowiązków innych osób (art. 29 ust 2 u.o.d.o.). Co istotne, w tym drugim przypadku administrator danych był zobowiązany do dokonania samodzielnej oceny „wiarygodności" i „potrzeby" posiadania konkretnych danych osobowych. Zła ocena owych przesłanek mogła spotkać się z konsekwencjami karnymi przewidzianymi w art. 51 u.o.d.o. (grzywna, ograniczenie wolności lub pozbawienie wolności do lat 2). Posiadając konkretne dane (numer IP, nazwę komputera, adres poczty elektronicznej, imię i nazwisko) uprawniony mógł dochodzić swoich roszczeń. Wskazana droga była często wykorzystywana, uznana za efektywną i wielokrotnie pojawiała się w orzeczeniach sądowych[22].

W nowelizacji u.o.d.o. z dnia 2010.12.06[23] uchylony został, omawiany wcześniej art. 29. W uzasadnieniu stwierdzono, iż związane jest to z dalszą implementacją Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady[24], a co za tym idzie, dostosowania prawa polskiego do regulacji unijnych[25]. Wobec tego wydaje się, że jedyną możliwością na zdobycie danych osobowych osoby naruszającej prawa powoda, jest posłużenie się przepisami Ustawy o Świadczeniu Usług Drogą Elektroniczną[26].

W przypadku gdy dana sprawa prowadzona jest przez organy państwowe (policja, prokuratura, rzecznik praw obywatelskich i in.) art. 18 ust 6 u.ś.u.d.e. nakłada na usługodawcę obowiązek udzielenia mu wszelkich informacji o zebranych danych osobowych, niezbędnych dla prowadzonych przez niego postępowań[27]. Niniejsza ustawa nie daje już tak wyraźnego uprawnienia podmiotom cywilnym. Osoby te mogą żądać ujawnienia danych osobowych innych podmiotów na podstawie art. 21 ust 1 u.ś.u.d.e. Zgodnie z nim usługodawca może po otrzymaniu

[15] Art. 488 par. 2 k.p.k. in finem

[16] Art. 308 k.p.k.

[17] Pseudonim jest elementem indywidualizującym daną osobę i podlega takiej samej ochronie jak imię i nazwisko. Jednak nie wyklucza to możliwości posiadania takiego samego pseudonimu przez więcej niż jedną osobę. W opisywanej sytuacji „dochodzenie" do konkretnej osoby po pseudonimie, mogłoby doprowadzić do pozwania złej osoby. Por. Filmmaker tracks down pirate bay user, takes him to court http://torrentfreak.com/filmmaker-tracks-down-pirate-bay-user-takes-him-to-court-100621/ [dostęp 24.03.2013]

[18] Wszelkie „ślady" które pozostawia użytkownik Internetu, korzystając z jego usług. Jest to przede wszystkim adres IP, będący niejako adresem danego komputera w Sieci, maska podsieci, rodzaj wykorzystywanej przeglądarki internetowej, adres poczty elektronicznej i in.

[19] Por. GIODO http://www.giodo.gov.pl/319/id_art/2258. [dostęp 02.05.2013]

[20] Dostawca danej usługi – podmiot odpowiedzialny za możliwość korzystania z danej usługi Internetowej np. poczty elektronicznej, hostingu plików, administrator strony internetowej (por. J. Gołaczyński (red.), Ustawa o świadczeniu usług drogą elektroniczną Komentarz, Warszawa 2009, s. 126)

[21] Ustawa z dnia 29 sierpnia 1997 r. o Ochronie Danych Osobowych. (Dz.U. 1997 nr 133 poz. 883)

[22] Por. wyrok SO we Wrocławiu z 23 07.2010 r. (I C 144/10), P. Waglowski „Super negatyw" – odpowiedzialność platformy aukcyjnej za komentarze użytkowników, http://prawo.vagla.pl/node/7435 [dostęp 22.04.2013]

[23] Dz.U.2010.229.1497

[24] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych

[25] K. Kaczmarek, Nowelizacja ustawy o ochronie danych osobowych, http://blog-daneosobowe.pl/?p=364 [dostęp 02.05.2013]

[26] Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną. (Dz.U. 2002 nr 144 poz. 1204)

[27] J. Gołaczyński (red.), Ustawa o świadczeniu…, s. 146

wiarygodnych wiadomości o korzystaniu przez usługobiorcę z usługi świadczonej drogą elektroniczną w sposób niezgodny z przepisami prawa lub regulaminem, przetwarzać dane osobowe usługobiorcy w celu ustalenia jego odpowiedzialności. Przewidziana przez ustawę niezgodność z przepisami związana jest z całym obowiązującym prawem, w związku z tym bez wątpienia kwalifikuje się pod to także zbiór przepisów zawartych w Kodeksie Cywilnym[28]. Ustawodawca nakłada jednak obowiązek utrwalenia danych informacji naruszających przepisy prawa lub regulaminu, a wobec braku możliwości prewencyjnego utrwalania danych osobowych bez zgody uprawnionego, ich archiwizowanie może nastąpić dopiero po wystąpieniu naruszenia (zagrożenia) i otrzymaniu wiarygodnej o tym informacji[29]. Należy jednak wspomnieć o uregulowaniu z art. 19 ust. 2 pkt 3 u.ś.u.d.e., które wyraźnie wskazuje, że dane osobowe mogą być przetwarzane także po zakończeniu trwania usługi, dla celów wyjaśnienia okoliczności przewidzianych w art. 21 ust. 1 u.ś.u.d.e. Sam art. 21 u.ś.u.d.e. gwarantuje możliwość uzyskania danych danej osoby, lecz zgodnie z zasadami art. 19 ust 1 u.ś.u.d.e., po zakończeniu korzystania z usługi przez usługobiorcę, dane nie ulegają dalszemu przetwarzaniu. Wyłomem w tym uregulowaniu jest wspomniany już art. 19 ust. 2 u.ś.u.d.e., który gwarantuje zachowanie i zabezpieczenie danych usługobiorcy naruszającego prawo do czasu wyjaśnienia spornych kwestii.

Powyższe rozważania wskazują jedną z dróg dochodzenia swoich praw na gruncie prawa cywilnego. Słowem zakończenia warto zauważyć, iż użytkownicy często błędnie kierują swoje roszczenia w stronę dostawców usług. Zgodnie z art. 14 u.ś.u.d.e. mogą oni bez problemów zostać zwolnieni z ponoszenia odpowiedzialności prawnej[30], a twierdzenie, że powinni ponosić odpowiedzialność za działania usługobiorców jest oczywiście błędne.

4. Zakończenie

Przy zastosowaniu odpowiednich przepisów można dotrzeć do niemal każdego użytkownika Sieci, zwłaszcza jeżeli dopuszcza się naruszania prawa. Droga ta jest jednak długa i kręta, a jej ciężar przerzucony niejednokrotnie na pokrzywdzonego. Wydaje się, że pomimo utworzenia wyłomów w prawie i zagwarantowania możliwości dochodzenia swoich roszczeń, prawo nadal bardziej faworyzuje sprawcę niż poszkodowanego. Mimo to ciężko wyważyć oba stanowiska, a praktyka stosowania wskazanych rozwiązań (w Internecie) jest zbyt krótka, by można było ją sprawiedliwie ocenić.

Nie zawsze jednak można odnaleźć adresata roszczeń. Korzystanie z *hot-spotów*, kawiarenek internetowych, zabezpieczanie się oprogramowaniem szyfrującym, korzystanie z sieci TOR czy w końcu z różnych serwerów *proxy* zapewnia bezpieczeństwo podmiotom naruszającym prawo. Wszelkie próby wprowadzenia ograniczenia prywatności, monitoringu sieci, akcje wymierzone przeciwko „internetowej złotej wolności" mogą spotkać się z ogromnymi akcjami protestacyjnymi[31] i z góry skazane są na porażkę.

[28] Ibidem s. 156

[29] J. Gołaczyński (red.), Ustawa o świadczeniu…, s. 157

[30] A. Wojciechowska, Naruszenie powszechnych dóbr osobistych w Internecie. [w:] Barta J., Markiewicz R., Media a dobra osobiste, Warszawa 2009 r., s. 390, oraz J. Gołaczyński (red.), Ustawa o świadczeniu…, s. 136

[31] Doskonałym przykładem takiej sytuacji są protesty mające miejsce przeciwko planowanemu wprowadzeniu Anti-Counterfeiting Trade Agreement w styczniu 2012 roku.

Abstract

Marcin Szurpicki in his article "Anonymity in the Web, or how to get to the subject of law infringement in the Internet", shows the problem of finding concrete person, responsible for legal infringement in the Web. Author proposes two possible ways of claiming the rights. In the first part he presents activities on the ground of criminal law with emphasis on private indictment. In the second part he concentrates on the civil law, shoving what plaintiff is able to do, to get access to the personal data of subject suspected of breaking the law. In the conclusion he claims that there are still situations in which the aggrieved is unable to find person responsible for infringement, however there is no effective solution of this problem.

Bibliografia

Banasiak Z., Przyjęcie zawiadomienia o przestępstwie prywatnoskargowym w praktyce policyjnej, [w:] Prokuratura i Prawo 7-8 2010, Kraków 2010,

Gołaczyński J. (red.), Ustawa o świadczeniu usług drogą elektroniczną Komentarz, Warszawa 2009

Grzegorczyk T., Kodeks postępowania karnego. Komentarz Warszawa 2006,

Grzegorczyk T., Tylman J., Polskie postępowanie karne, Warszawa 2009,

Wojciechowska A., Naruszenie powszechnych dóbr osobistych w Internecie. [w:] Barta J., Markiewicz R., Media a dobra osobiste, Warszawa 2009 r.

HONORATA ZARĘBSKA

POPRAWA DOSTĘPNOŚCI INFORMACJI O ORZECZNICTWIE SĄDOWYM W INTERNECIE[1]

Współczesne zautomatyzowane systemy informacji o orzecznictwie sądowym adresowane do obywateli wpisują się coraz częściej w kategorię zasobów internetowych. Przynajmniej w teorii, może z nich bezpłatnie skorzystać każda osoba posiadająca komputer lub inne urządzenie obsługujące World Wide Web. Idea udostępniania informacji o rozstrzygnięciach sądów w ten sposób jest jak najbardziej słuszna i pożyteczna, gdyż jak stwierdza Grzegorz Wiaderek: „nie można (…) uznać, iż publikacje w drukowanych zbiorach orzecznictwa czy publikacje w komercyjnych programach komputerowych są wystarczające"[2]. Kwestia realnej dostępności tego typu informacji jest jednak znacznie bardziej skomplikowana. Nie może być ona jednak rozpatrywana wyłącznie przez pryzmat liczb, określających kto i w jakim stopniu korzysta lub nie korzysta z Internetu, komputera, systemu, gdyż docelowo każdy system informacji adresowany do obywatela – lub finansowany ze środków publicznych – powinien być zaprojektowany w sposób uwzględniający możliwie najszerszy krąg odbiorców.

Na świecie niestety do rzadkości należą niekomercyjne systemy, w których uwzględniono potrzeby użytkowników wymagających – z różnych względów – odmiennego sposobu dotarcia do informacji zgromadzonych w systemie[3]. Są to m.in.:

- osoby niepełnosprawne[4], tj. z zaburzeniami neurologiczno-kognitywnymi, motorycznymi oraz z dysfunkcjami słuchu, wzroku[5];
- seniorzy;
- analfabeci;
- użytkownicy napotykający ograniczenia technologiczne i związane z kompatybilnością (przeglądarek, systemów operacyjnych, urządzeń, itp.);
- użytkownicy ograniczeni przez warunki środowiskowe (miejsce, wolne łącze internetowe, itp.)[6].

Dominik Paszkiewicz podaje, że w skrajnych sytuacjach lekceważenie zasad dostępności w projektowaniu systemów może stać się nawet źródłem zagrożenia zdrowia dla użytkowników. Na przykład osoby chore na padaczkę w odmianie fotogennej nie powinny oglądać migających elementów na stronie internetowej. Rozwiązanie tego typu nie jest również właściwe dla osób z zaburzeniami koncentracji, widzenia i dyslektyków[7].

Projektowanie uniwersalne

Koncepcję projektowania produktów, usług, otoczenia w taki sposób, aby mogły być one wykorzystywane przez jak największe grono ludzi (bez względu na wiek, możliwości i sytuację), bez konieczności specjalistycznego ich adaptowania oraz z uwzględnieniem estetyki wykonania, określa się mianem „projektowania uniwersalnego" (z ang. *universal design, universal access, design for all*)[8] albo „projektowaniem bez barier" (z ang. *barier-free design*)[9]. Najważniejsze zasady projektowania uniwersalnego zaproponowane przez Center for Universal Design prezentuje Tabela 1.

Tabela 1. Zasady projektowania uniwersalnego w komputerowych systemach informacji

Zasada	Opis
Równość w użytkowaniu (z ang. *equitable use*)	System powinien być dostosowany do różnorodnych potrzeb użytkowników zarówno w zakresie sposobu pracy z systemem jak i formy prezentacji zasobów. Nie można jednak tworzyć osobnych, wyłączonych narzędzi i zbiorów informacji dedykowanych użytkownikom ze specjalnymi potrzebami.
Elastyczność użycia (z ang. *flexibility in use*)	Użytkownik powinien mieć możliwość personalizacji pracy z systemem oraz wyboru formy prezentacji informacji o zasobach (na przykład zamieniać formę tekstową na audialną) .
Prosta i intuicyjna obsługa (z ang. *simple and intuitive*)	Praca z systemem nie może być uzależniona od posiadania przez użytkownika zaawansowanych kompetencji informacyjno-komunikacyjnych oraz wiedzy fachowej. Należy unikać rozwiązań skomplikowanych i nieintuicyjnych.
Zauważalna informacja (z ang. *perceptible information*)	System powinien gwarantować taki układ treści, w którym ważne informacje są eksponowane i możliwe do odczytania na różne sposoby (wiąże się to również z poprawnością kodu).

[1] Projekt został sfinansowany ze środków Narodowego Centrum Nauki przyznanych na podstawie decyzji numer DEC-2011/01/N/HS2/01062.

[2] G. Wiaderek: Powszechny dostęp do aktów prawnych i orzeczeń sądowych. W: Powszechny dostęp do aktów prawnych i orzecznictwa: prawo i praktyka [dok. elektr.]. Red. B. Gruszka. Warszawa 2011, s. 3-9. Dokument dostępny w Internecie: http://www.isp.org.pl/uploads/pdf/1671383281.pdf [dostęp: 4.15.2012]

[3] Analiza rozwiązań stosowanych w europejskich niekomercyjnych systemach informacji o orzecznictwie sądowym jest jednym z elementów realizowanej przez autorkę rozprawy doktorskiej.

[4] Szacuje się, że osoby niepełnosprawne stanowią od 10% do 15% populacji Europy, czyli od około 50 do 75 milionów ludzi w 27 krajach Unii Europejskiej (Eurostat, 2002).

[5] How People with Disabilities Use the Web. Overview [dok. elektr.]. Ed. S. Abou-Zahra [i in.]. Dokument dostępny w Internecie: http://www.w3.org/WAI/intro/people-use-web/ [dostęp: 20.11.2012].

[6] Web Accessibility [dok. elektr.]. Dokument dostępny w Internecie: http://ec.europa.eu/ipg/standards/accessibility/index_en.htm [dostęp: 20.11.2012].

[7] D. Paszkiewicz: Jak zrobić dostępną stronę internetową: poradnik dla projektantów i redaktorów [dok. elektr.]. Warszawa 2011, rozdz. 2.13. Dokument dostępny w Internecie: http://www.undp.org.pl/ content/download/932/5301/file/Dost%C4%99pne%20strony%20-%20poradnik.pdf [dostęp: 25.11.2012].

[8] M. Fedorowicz: Projektowanie uniwersalne. Implementacja w obszarze edukacji i bibliotekarstwa szkolnego. „Przegląd Biblioteczny" 2007 z. 3 s. 400.

[9] Idea projektowania uniwersalnego zaczęła się rozwijać na początku lat sześćdziesiątych w Stanach Zjednoczonych. Jej autorem jest Ronald Mace, architekt poruszający się na wózku inwalidzkim.

Tolerancja dla błędów (z ang. *tolerance for error*)	System powinien posiadać rozwiązania, które eliminują lub minimalizują ryzyko popełnienia błędu przez użytkownika w trakcie pracy z systemem (instrukcje obsługi, podpowiedzi, możliwość cofnięcia operacji, itp.)
Niski poziom wysiłku fizycznego (z ang. *low physical effort*)	Efektywna praca z systemem nie może wymagać od użytkownika zbytniego wysiłku fizycznego (na przykład zmęczenia oczu).
Odpowiednie środowisko użycia (z ang. *size and space for approach and use*)	Każdy element systemu (obiekt, proces) powinien być dostępny dla każdego użytkownika bez względu na jego warunki fizyczne, warunki pracy oraz możliwości technologiczne. Wiąże się to między innymi z zapewnieniem pracy z systemem na różnych urządzeniach oraz przy użyciu różnorodnego oprogramowania.

Źródło: M. Story: *The Principles of Universal Design…*[10]

Realizację powyższych zasad można dostrzec w niektórych zagranicznych zautomatyzowanych systemach informacji o orzecznictwie. Szkoda, ponieważ zastosowanie standardów dostępności w wielu przypadkach nie powoduje dużego wysiłku dla projektantów. Już rezygnacja z technologii Flash czy DHTML-a oraz nadmiernego „bombardowania" użytkownika różnorodnością opcji i kolorów jest dużym krokiem w kierunku zwiększenia uniwersalności systemu.

W dalszej perspektywie warto również zwrócić uwagę na możliwości udostępniania informacji o orzecznictwie za pomocą urządzeń mobilnych. Jak wiadomo, urządzenia te pozwalają połączyć się z Internetem w dowolnym miejscu pobytu użytkownika. Jak pokazują badania, liczba osób wykorzystujących urządzenia mobilne w ten sposób, stale rośnie[11]. Tendencję tę dostrzegli twórcy austriackiego systemu RIS Rechtsinformationssystem des Bundes i zaprojektowali interesującą aplikację RIS:App umożliwiającą korzystanie z systemu RIS na urządzeniach mobilnych (smartfonach i tabletach). Działa ona w systemie operacyjnym iOS[12]. Co ciekawe, Austriacy stworzyli również specjalną aplikacją-nakładką umożliwiającą pracę z tekstami decyzji sądowych w środowisku popularnego edytora Microsoft Word, w tym przede wszystkim eksport materiałów do edytora. Nosi ona nazwę RIS Recherche für Microsoft Word. Aplikacje powstały w wyniku współpracy sektora nauki, biznesu oraz rządu, a dokładniej Biura Kanclerza Federalnego Austrii, firmy Right2Innovation oraz Uniwersytetu w Salzburgu.

W holenderskim systemie Rechtspraak użytkownik może natomiast samodzielnie pobierać przygotowywane raz dziennie aktualizacje w postaci skompresowanych pakietów orzeczeń opisanych za pomocą XML w dogodnym dla siebie czasie. Jest to istotne w momencie, gdy posiada on na przykład ograniczony dostęp do Internetu. Zastosowane rozwiązanie umożliwia mu łatwe zarządzanie tymi informacjami w trybie off-line oraz łatwe włączanie treści pobranych z systemu do prywatnej bazy danych.

Ogólny przegląd rozwiązań w zakresie dostępności spotykanych w zautomatyzowanych systemach informacji o orzecznictwie sądowym prezentuje Tabela 2.

Tabela 2. Przegląd rozwiązań w zakresie web accessibility

Opcja	Opis
„Mówiąca strona"	Możliwość odsłuchania zawartości strony internetowej przy pomocy wbudowanego syntezatora mowy albo możliwość zapoznania się z treścią strony w języku migowym.
Przyciski do powiększania czcionki	Niewielu użytkowników wie, że z poziomu przeglądarki można dowolnie zmieniać wielkość tekstu. Dla tych osób istnieją specjalnie wyeksponowane przyciski, najczęściej oznaczone znakami: „+", „-", „0" (albo „reset") umożliwiające szybkie dostosowanie rozmiaru czcionki do potrzeb: powiększenie, zmniejszenie lub powrót do ustawień domyślnych.
Alternatywna wersja kolorystyczna	Opcja umożliwiają wyświetlenie strony w innej wersji kolorystycznej, na przykład w wersji z odwróconymi kolorami (wersja negatywowa). W tym celu można zastosować różne style CSS (z ang. *Cascading Style Sheets*) .
Skróty klawiaturowe (z ang. *access keys*)	Kombinacje klawiszy (zwykle są to klawisze funkcyjne) przystosowane do obsługi strony internetowej, zwykle związane z nawigacją (skróty do odnośników, formularzy, itp.). Udogodnienie to musi być stosowane z rozwagą, ponieważ może kolidować ze skrótami przewidzianych w przeglądarkach lub aplikacjach czytających (z ang. *screen readers*).
Alternatywna wersja tekstowa (z ang. *easy read format*)	Niektóre systemy udostępniają informacje w wersji uproszczonej. Krótkie akapity tekstu są wzbogacane o symboliczne elementy graficzne obrazujące treść. Struktura alternatywnej wersji językowej musi być czytelna a język przekazu bezpośredni i prosty (najlepiej kiedy jedno zdanie opisuje jedną myśl). W niektórych systemach stosuje się określenie tekst wolny od żargonu (z ang. *jargon free text*).
Łatwa nawigacja	Spójna, intuicyjna i zrozumiała nawigacja daje użytkownikowi możliwość szybkiego odnalezienia się w hierarchii zasobów. Powinno dać się ją obsłużyć z poziomu klawiatury. Ważne elementy wygodnej nawigacji to: – dobrze oznaczone i logicznie uporządkowane, niezbyt głębokie i niezbyt długie menu, – fokus (obramowanie na aktywnym elemencie strony), – zmiana koloru hiperłącz przy interakcji, – bezpośrednie odnośniki umożliwiające szybkie przejście do określonego elementu (na przykład na górę strony, na dół strony, do treści, do wyszukiwarki), w tym również nawigacja łańcuszkowa.

Źródło: D. Paszkiewicz: *Dostępność serwisów internetowych…*[13]

Projektowanie włączające

Na uwagę zasługuje również podejście określane mianem projektowania włączającego (z ang. *inclusive design*)[14]. Zwraca się w nim uwagę na konieczność poznania oczekiwań i potrzeb jak największej grupy potencjalnych użytkowników w celu zapobieżenia ich wykluczeniu[15]. Okazuje się, że potrzeby te można uporządkować hierarchicznie i odnieść do jakiegokolwiek produktu, usługi, otoczenia, a zatem również do zautomatyzowanych systemów informacji o orzecznictwie (zob. Rysunek 1).

[10] M. Story: The Principles of Universal Design. W: Universal Design Handbook. Eds. W. Preiser [i in.]. New York 2010, Rozdział 3.4.

[11] Na przykład w Polsce w 2006 r. było to 0,7% spośród wszystkich ankietowanych w wieku 16-74, a w 2012 r. już 4,5% ankietowanych. Więcej na ten temat, zob. Digital Agenda Scoreboard key indicators [dok. elektr.]. Dokument dostępny w Internecie: http://digital-agenda-data.eu/charts/see-the-evolution-of-an-indicator-and-compare-countries [dostęp: 18.09.2013]

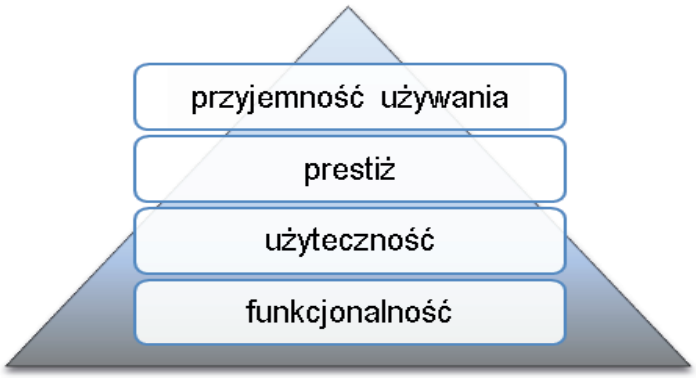
[12] Wkrótce ma się pojawić wersja dla systemu Android.

[13] D. Paszkiewicz: Dostępność serwisów internetowych. Podręcznik na temat dobrych rozwiązań w projektowaniu dostępnych serwisów internetowych dla osób z różnymi rodzajami niepełnosprawności. Warszawa 2011.

[14] Podejście to zostało również dostrzeżone przez Komisję Europejską. Komisja podkreśla rolę ICT jako czynnika wspierającego integrację społeczną i podnoszącego jakość życia oraz podejmuje działania na rzecz „społeczeństwa informacyjnego dla wszystkich" poprzez promowanie integracyjnego społeczeństwa cyfrowego (inclusive digital society), które daje wszystkim szanse oraz minimalizuje ryzyko wykluczenia.

[15] K. Best: Design Management. Managing Design Strategy, Process and Implementation. Lausanne 2006, s. 208.

Rysunek 1. Hierarchia potrzeb użytkowników w projektowaniu włączającym



Źródło: na podstawie J. de Souza van der Linden, C. Fischer Brendler: The Hierarchy of Needs to Inclusive Design… [16]

Badania nad projektowaniem włączającym pokazują, że użytkownikowi najbardziej zależy na funkcjonalności (z ang. *funcionality*). System musi działać w sposób określony przez twórców oraz być pozbawiony błędów. W dalszej kolejności oczekuje on, że system będzie użyteczny (z ang. *usability*), czyli łatwy w użyciu, intuicyjny, przyjazny (z ang. *user-friendly*). Okazuje się, że odbiorca jest w stanie tolerować system niespełniający wymogów użyteczności, o ile zostanie zaspokojona podstawowa potrzeba funkcjonalności. W kontekście włączania potrzeb odbiorcy niestandardowego ważne jest również, aby system był znaczący (z ang. *dignity*), nie odstawał pod względem jakości, profesjonalizmu od innych systemów. Chodzi o to, aby użytkownik nie odczuwał dyskomfortu związanego z podziałem systemów na systemy dla użytkowników standardowych i systemy dla użytkowników niestandardowych. Ostatnie miejsce w hierarchii zajmuje potrzeba przyjemności (z ang. *pleasure*) związana z doświadczeniem użytkownika (z ang. *user experience*) podczas pracy z systemem. W sytuacji, kiedy istnieje kilka znaczących systemów o podobnej funkcjonalności i użyteczności użytkownik wybierze ten, który jest dla niego najbardziej atrakcyjny.

Wytyczne web accessibility

Projektanci mają do dyspozycji różne standardy opisujące, w jakim kierunku powinni oni działać na rzecz poprawy dostępności systemów. W tym kontekście warto zwrócić uwagę na działalność najbardziej opiniotwórczej – w zakresie projektowania uniwersalnego związanego ze środowiskiem internetowym – organizacji World Wide Web Consortium (W3C), zajmującej się między innymi projektowaniem standardów. W ramach jednej z sekcji W3C funkcjonującej pod nazwą Web Accessibility Initiative (WAI)[17] powstał zbiór zasad, jakimi powinni się kierować projektanci i redaktorzy zasobów internetowych pod tytułem *Web Content Accessibility Guidelines* (w skrócie WCAG). 15 października 2012[18] roku uzyskały one status międzynarodowej normy *ISO/IEC 40500:2012 Information technology -- W3C Web Content Accessibility Guidelines (WCAG) 2.0*[19].

Do tej pory sekcja WAI wydała dwie wersje wytycznych WCAG. 5 maja 1999 roku wyszła pierwsza wersja wytycznych WCAG 1.0[20]. Kolejna – zmieniona i dostosowana do nowych realiów technologicznych – została opublikowana 11 grudnia 2008 roku pod nazwą WCAG 2.0[21]. Kluczowe zasady dostępności zaproponowane tej wersji prezentuje Tabela 3.

Tabela 3. Cztery zasady dostępności według WCAG 2.0[22]

Możliwość odbioru (z ang. *perceivable*)
Informacja oraz elementy interfejsu muszą zostać zaprezentowane w sposób możliwy do odbioru przez użytkownika. Wiąże się to z: – zastosowaniem alternatywnego przekazu zawartości (na przykład opis tekstowy obrazów, napisy zsynchronizowane z materiałem wideo lub tłumaczenie na język migowy, itp.); – rozdzieleniem warstwy treści (zawierającej informacje) od warstwy prezentacji (wyglądu, fizycznego kształtu i stylu); – wyeksponowaniem informacji pierwszoplanowych od tła (na przykład poprzez umożliwienie użytkownikowi samodzielnej zmiany rozmiaru czcionki lub kontrastu bez utraty funkcjonalności serwisu internetowego).
Operacyjność (z ang. *operable*)
Wszystkie składniki interfejsu użytkownika oraz nawigacja powinny być zaprojektowane w taki sposób, aby użytkownik mógł je obsługiwać wyłącznie przy użyciu klawiatury, bez ograniczeń czasowych wynikających na przykład z powodu wygaśnięcia autoryzacji oraz z zachowaniem zasad bezpieczeństwa (zawartość nie może wywoływać stanów napadowych u użytkownika, na przykład padaczkowych). Należy również zadbać o łatwą nawigację i wyszukiwanie informacji oraz o możliwość szybkiego ustalenia położenia na stronie.
Zrozumiałość (z ang. *understandable*)
Wszystkie informacje zamieszczone na stronie oraz sposób działania interfejsu muszą być zrozumiałe dla użytkownika. Teksty powinny być czytelne i łatwe do zrozumienia, zaś sama strona powinna reagować na działania użytkownika w przewidywalny sposób. Dodatkowo powinny istnieć narzędzia wsparcia użytkownika dotyczące jego interakcji z systemem, które eliminują i minimalizują ryzyko pojawienia się błędów oraz umożliwiają ich szybką korektę (instrukcje, podpowiedzi, wyszukiwanie rozmyte, możliwość cofnięcia przesłania danych, itp.) .
Kompatybilność (z ang. *robust*)
Strona powinna być niezależna od technologii wykorzystywanej przez użytkownika oraz powinna współdziałać z narzędziami pomocniczymi (na przykład ze skryptami). Jeśli jest to niemożliwe należy tworzyć dostosowane do potrzeb wersje alternatywne strony.

W ostatnich latach wiele państw i instytucji międzynarodowych zainteresowało się projektowaniem uniwersalnym, czego efektem jest wprowadzenie przepisów regulujących kwestie techniczne w zakresie dostępności informacji finansowanych ze środków publicznych. Chodzi o przystosowanie komputerowych systemów informacji publicznej do zróżnicowanych potrzeb członków życia społecznego. Na szeroką skalę stosuje się zwłaszcza zalecenia WCAG.

Rezolucja Rady w sprawie planu działania eEuropa 2002: dostępność publicznych stron internetowych i ich zawartości[23] wprowadziła standaryzację w zakresie dostępności stron inter-

[16] J. de Souza van der Linden, C. Fischer Brendler: The Hierarchy of Needs to Inclusive Design. "Work A Journal of Prevention, Assessment and Rehabilitation" 2012 vol. 41 suppl. 1 s. 1360.

[17] Web Accessibility Initiative [dok. elektr.]. Dokument dostępny w Internecie: http://www.w3.org/WAI/ [dostęp: 20.11.2012].

[18] W3C Web Content Accessibility Guidelines 2.0 Approved as ISO/IEC International Standard [dok. elektr.]. Dokument dostępny w Internecie: http://www.w3.org/2012/07/wcag-2pas-pr.html [dostęp: 20.11.2012]

[19] Pełna treść normy w wolnym dostępie znajduje się na stronie W3C.

[20] Web Content Accessibility Guidelines 1.0: W3C Recommendation 5-May-1999 [dok. elektr.]. Eds. W. Chisholm, G. Vanderheiden, I. Jacobs. Dokument dostępny w Internecie: http://www.w3.org/TR/WCAG10/ [dostęp: 20.11.2012].

[21] Web Content Accessibility Guidelines (WCAG) 2.0: W3C Recommendation 11 December 2008 [dok. elektr.]. Eds. B. Caldwell [i in.]. Dokument dostępny w Internecie: http://www.w3.org/TR/WCAG/ [dostęp: 20.11.2012].

[22] Tamże.

[23] Council Resolution of 25 March 2002 on the eEurope Action Plan 2002: accessibility of public websites and their content. Dz.U. Unii Europejskiej C 86, 10.4.2002.

netowych oficjalnych instytucji na poziomie WCAG 1.0 A[24]. Od stycznia 2010 roku wszystkie unijne serwisy powinny być zgodne z nowszymi wytycznymi WCAG 2.0 na wyższym poziomie AA. Jest to jeden z elementów strategii na rzecz rozwoju społeczeństwa i zapewnienia wszystkim obywatelom równego dostępu do informacji. Unia wzywa również państwa członkowskie do wspierania działań mających na celu znaczne zwiększenie w Europie gamy dostępnych produktów i usług o charakterze informacyjno-komunikacyjnym.

W efekcie, w wielu krajach tworzenie oficjalnych państwowych serwisów internetowych w zgodzie z WCAG staje się obowiązkiem. Wdraża się albo oryginalne zalecenia WCAG, albo ich zmodyfikowane (przystosowane do krajowych realiów) wersje. Przegląd zagranicznych rządowych wytycznych w zakresie dostępności prezentuje Tabela 4.

Tabela 4. Przegląd zagranicznych wytycznych w zakresie web accessibility

Kraj	Nazwa standardu	Opis
Czechy	Pravidla pro tvorbu přístupných webových stránek	Na podstawie ustawy o systemach informacyjnych administracji publicznej[25] w 2004 roku sformułowano pierwsze zalecenia w zakresie dostępności. Po fali krytyki przeformułowano je dwukrotnie i obecnie obowiązuje wersja z 2008 roku[26]. Zasady opierają się na WCAG 2.0 i składają się z 33 wytycznych podzielonych na 6 obszarów tematycznych.
Francja	Référentiel général d'accessibilité pour les administration RGAA 2.2.1	W wyniku prac nad zapewnieniem osobom niepełnosprawnym równego dostępu do informacji we Francji wprowadzono *Ogólne zasady dostępności administracji (RGAA)*[27], które dotyczą trzech kanałów dystrybucji informacji publicznej: Internetu, telewizji i telefonii. Dostępność serwisów internetowych regulują obecnie wytyczne zawarte w wersji RGAA 2.2.1 z listopada 2009 roku oparte na WCAG 2.0. Podstawą prawną powyższych działań jest ustawa o równych prawach, szansach, uczestnictwie i obywatelstwie osób niepełnosprawnych[28].
Niemcy	Barrierefreie-Informationstechnik-Verordnung - BITV 2.0	Obecnie, na mocy rozporządzenia z 12 września 2011 roku[29], w oficjalnych państwowych serwisach internetowych stosuje się nieznacznie zmodyfikowane zalecenia WCAG 2.0. Wymagania ograniczają się do dwóch a nie trzech priorytetów (Priorytet 1 i Priorytet 2). Najnowsze zmiany dotyczą wprowadzenia udogodnień w zakresie przekazywania informacji za pośrednictwem języka migowego (muszą zostać wprowadzone do marca 2014 roku)[30]. Podstawą prawną powyższych działań jest ustawa o równości osób niepełnosprawnych[31].
Irlandia	WCAG 1.0	Ustawa o niepełnosprawności[32] jest ważnym elementem programu ramowego rządu irlandzkiego na rzecz integracji społecznej i podstawą prawną dla działań na rzecz zwiększania dostępności informacji finansowanej ze środków publicznych w Internecie. Działania te są koordynowane przez Krajowy Urząd ds. Niepełnosprawnych (z ang. *National Disability Authority,* NDA). NDA opracowało zestaw 14 wytycznych oraz 41 kryteriów w zakresie dostępności (w tym związane z ICT)[33]. Instytucje są zobligowane do stosowania WCAG 1.0 na poziomie AA.
Holandia	Webrichtlijnen 2.0	23 czerwca 2011 roku Komitet Normalizacyjny (*College Standaardisatie*) przyjął nową wersję wytycznych dotyczących dostępności rządowych serwisów w Internecie (opublikowana 1 lipca 2011 roku), która częściowo opiera się na standardzie WCAG 2.0[34]. Zwrócono w nich uwagę między innymi na możliwość odbioru informacji przy pomocy nowoczesnych urządzeń (smartfon, tablet, itp.). Istniejące serwisy zgodne z WCAG 1.0 mają czas do 2014 roku na wprowadzenie modyfikacji WCAG 2.0. System informacji o orzecznictwie uzyskał certyfikat dostępności zasobów wystawiany przez Fundację na Rzecz Dostępności (z ang. *Stichting Accessibility*).
Hiszpania	UNE 139803:2012	4 lipca 2012 roku hiszpański krajowy komitet normalizacyjny AENOR (z hiszp. *Asociación Española de Normalización y Certificación*) wydał nową wersję regulacji w sprawie dostępności serwisów internetowych UNE 139803:2012[35] oparta na WCAG 2.0. Zastąpiła ona normę UNE 139803:2004[36] bazującą na WCAG 1.0. Dwa najważniejsze hiszpańskie akty prawne z zakresu e-dostępnością to: ustawa dotycząca usług społeczeństwa informacyjnego i handlu elektronicznego wydana w 2002 roku[37] oraz ustawa w sprawie równych szans, powszechnej dostępności i niedyskryminowania osób niepełnosprawnych[38]. Na ich podstawie w grudniu 2005 usankcjonowano obowiązek dostosowania stron internetowych instytucji państwowych z zachowaniem standardów dostępności.
Wielka Brytania	BS 8878:2010	W grudniu 2010 roku Brytyjski Instytut Normalizacyjny (z ang. *British Standards Institution*) wydał normę BS 8878:2010[39] (zastąpiła specyfikację PAS 78:2006[40]). Wytyczne są realizacją przepisów o przeciwdziałaniu dyskryminacji osób niepełnosprawnych zawartych w ustawie o równości[41] (dokładniej w rozdziale 25 poświęconym usługom społeczeństwa informacyjnego) oraz rządowych działań w ramach e-Accessibility Action Plan[42]. Norma zaleca tworzenie stron internetowych zgodnych z WCAG 2.0 na poziomie AA.

[24] Polityka dostępności sieci [dok. elektr.]. Dokument dostępny w Internecie: http://europa.eu/geninfo/accessibility_policy_pl.htm [dostęp: 20.11.2012].

[25] Zákon ze dne 14. září 2000 o informačních systémech veřejné správy a o změně některých dalších zákonů. Sbírka zákonů částka 99 číslo 365, 14.09.2000.

[26] Zasady są załącznikiem do rozporządzenia Vyhláška ze dne 7. února 2008 o formě uveřejňování informací souvisejících s výkonem veřejné správy prostřednictvím webových stránek pro osoby se zdravotním postižením (vyhláška o přístupnosti). Sbírka zákonů částka 20 číslo 64, 07.02.2008.

[27] Référentiel Général d'Accessibilité pour les Administrations RGAA: v. 2.2.1 [dok. elektr.]. Dokument dostępny w Internecie: http://www.references.modernisation.gouv.fr/sites/default/files/RGAA_v2.2.1.pdf [22.11.2012].

[28] Loi n° 2005-102 du 11 février 2005 pour l'égalité des droits et des chances, la participation et la citoyenneté des personnes handicapées. Journal Officiel de la République Française n°36 texte n°1, 12.02.2005.

[29] Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (Barrierefreie-Informationstechnik-Verordnung - BITV 2.0) vom 12. September 2011. Bundesgesetzblatt Jahrgang 2011 Teil I Nr. 48, 21.09.2011.

[30] Barrierefreie Informationstechnik-Verordnung (BITV) [dok. elektr.]. Dokument dostępny w Internecie: http://www.die-barrierefreie-website.de/barrierefrei/barrierefreie-informationstechnik-verordnung.html [dostęp: 20.11.2012].

[31] Gesetz zur Gleichstellung behinderter Menschen (Behindertengleichstellungsgesetz - BGG) vom 27. April 2002. Bundesgesetzblatt Jahrgang 2002 Teil I Nr. 28, 30.04.2002.

[32] Disability Act 2005 [dok. elektr.]. Acts of the Oireachtas 2005 no. 14. Dokument dostępny w Internecie: http://www.oireachtas.ie/documents/bills28/acts/2005/a1405.pdf [dostęp: 20.11.2012].

[33] Krajowy Urząd ds. Niepełnosprawnych wraz z Ministerstwem Sprawiedliwości przyznają corocznie nagrodę „Poprzez dostępność ku doskonałości" (Excellence Through Accessibility) instytucjom, które wyróżniają się w zakresie zwiększania dostępności różnych usług, produktów dla użytkowników niestandardowych.

[34] Webrichtlijnen versie 2 [dok. elektr.]. Dokument dostępny w Internecie: http://versie2.webrichtlijnen.nl/ [dostęp: 20.11.2012].

[35] Una Norma Española UNE 139803:2012 Requisitos de accesibilidad para contenidos en la Web. Madrid 2012.

[36] Una Norma Española UNE 139803:2004 Aplicaciones informáticas para personas con discapacidad. Requisitos de accesibilidad para contenidos en la Web. Madrid 2004.

[37] Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. Boletín Oficial del Estado nş 166, 12.07.2002.

[38] Ley 51/2003, de 2 de diciembre, de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad. Boletín Oficial del Estado nş 289, 03.12.2003.

[39] British Standard BS 8878 Web Accessibility. Code of Practice. London 2010.

[40] Publicly Available Specification PAS 78 Guide to Good Practice in Commissioning Accessible Websites. London 2006.

[41] Equality Act 2010. United Kingdom Public General Acts 2010 c[hapter] 15.

[42] The eAccessibility Action Plan: Making Digital Content Accessible by Everyone [dok. elektr.]. Dokument dostępny w Internecie: http://www.culture.gov.uk/images/publications/11-p110a-e-accessibility-action-plan-update-january-2011.pdf [dostęp: 20.11.2012].

W Polsce 31 maja 2012 roku weszło w życie rozporządzenie[43] zobowiązujące podmioty publiczne do stosowania wymagań WCAG 2.0 na poziomie AA przy tworzeniu serwisów informacyjnych. Jest ono aktem wykonawczym ustawy dotyczącej informatyzacji działalności podmiotów realizujących zadania publiczne[44]. Oznacza to, że internetowe systemy informacyjne z zakresu orzecznictwa powinny wkrótce się stać bardziej dostępne.

Podsumowanie

Zapewnienie dostępu do informacji o orzecznictwie dla wszystkich, w tym również osób z odmiennymi potrzebami w zakresie udostępniania informacji[45], powinno leżeć u podstaw tworzenia każdego systemu informacyjnego adresowanego do obywateli. W każdym innym przypadku jest to trudny do usprawiedliwienia przejaw dyskryminacji. W zakresie dostępności internetowej projektanci systemów mają do dyspozycji, przede wszystkim, ogólnodostępną międzynarodową normę *ISO/IEC 40500:2012 Information technology – W3C Web Content Accessibility Guidelines (WCAG) 2.0*[46]. Rządy wielu krajów wdrożyły wytyczne w zakresie web accessibility w odniesieniu do zasobów internetowych generowanych przez państwo dla obywateli. Można się spodziewać, że dostępność systemów informacji o orzecznictwie sądowym będzie się poprawiać w najbliższych latach, zwłaszcza że w wielu przypadkach wprowadzenie rozwiązań poprawiających dostępność nie wymaga specjalnych nakładów energii, czasu i kapitału.

Abstract

In her article entitled 'Improvement in accessibility of information about judicial decisions in the internet', Honorata Zarębska presents possibilities to access the information in question for the general public including those who have different needs related to availability of information. She provides examples of solutions that aim at supporting the design of accessibility systems and solutions that have been introduced by governments of numerous countries with regard to the Internet resources generate by the state for citizens. Additionally, she pays attention to opportunities for making information about judicial decisions available by means of mobile devices.

[43] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych. Dz.U. 2012 nr 0 poz. 526.

[44] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne. Dz.U. 2005 nr 64 poz. 565.

[45] Na przykład osoby niepełnosprawne, seniorów, analfabetów, użytkowników napotykających ograniczenia technologiczne i związane z kompatybilnością, użytkowników ograniczonych przez warunki środowiskowe i innych.

[46] Pełna treść normy w wolnym dostępie znajduje się na stronie W3C.